
2024
الثروات العالمية في التقرير
CROWDSTRIKE

مقدمة

يأتي إصدار عام 2024 من تقرير التهديدات العالمية الصادر عن شركة CrowdStrike في لحظة محورية بالنسبة لمجتمعنا العالمي من الحماة. تستمر سرعة وضراوة الهجمات الإلكترونية في التسارع مع قيام الخصوم بضغط الوقت بين الدخول الأولي والتحرك الجانبي والاختراق.

وفي الوقت نفسه، فإن صعود الذكاء الاصطناعي التوليدي لديه القدرة على خفض حاجز الدخول أمام الخصوم ذوي المهارات المنخفضة، مما يجعل من الأسهل إطلاق هجمات أكثر تطوراً وحداثة.

إن هذه الاتجاهات تدفع إلى تحول جذري في المشهد الأمني والعالم. إن النهج "الجيد بما فيه الكفاية" في التعامل مع الأمن السيبراني لم يعد كافياً لمواجهة التهديدات الحديثة. ومع انتقال المؤسسات بشكل متزايد إلى السحابة، يعمل الخصوم على تطوير قدراتهم على استغلال هذه الميزة وإساءة استخدام الميزات الفريدة للسحابة. ونستمر في رؤية الهجمات القائمة على الهوية تحتل مركز الصدارة، حيث يركز الخصوم على هجمات الهندسة الاجتماعية التي تتجاوز المصادقة متعددة العوامل.

إن استخدام الأدوات المشروعة لتنفيذ هجوم، وهي تقنية منتشرة بشكل متزايد، يعوق القدرة على التمييز بين

نشاط طبيعي وخرق.

نحن ندخل عصر سباق التسلح السيبراني حيث ستعمل الذكاء الاصطناعي على تضخيم التأثير لكل من متخصصي الأمن والخصم.

لا تستطيع المنظمات أن تتحمل التخلف عن الركب، والتكنولوجيا القديمة

إن ما كان في الماضي لا يقارن بالسرعة والتعقيد الذي كان عليه

الخصم الحديث.

مع إصدار تقرير التهديدات العالمية لعام 2024 من CrowdStrike، يقدم فريق عمليات مكافحة الخصوم المتميز لدينا المعلومات الاستخباراتية العملية التي تحتاجها للبقاء في طليعة التهديدات الحالية وتأمين مستقبلك. يقدم تقرير هذا العام رؤى وملاحظات بالغة الأهمية حول نشاط الخصوم، بما في ذلك:

- التكتيكات والتقنيات التي يستخدمها الخصوم للاستغلال فجوات في حماية السحابة

- الاستغلال المستمر لبيانات الهوية المسروقة وتستخدم الخصوم أساليب متطورة بشكل متزايد لتحقيق مكاسب. الوصول الأولي

- التهديد المتزايد لهجمات سلسلة التوريد والاستغلال من البرامج الموثوقة لتحقيق أقصى قدر من العائد على الاستثمار من الهجمات

- إمكانية استهداف الخصوم للانتخابات العالمية خلال عام واحد التي لديها القدرة على تحويل الجغرافيا السياسية حول العالم في المستقبل القريب

منذ اليوم الأول، قالت شركة CrowdStrike: "ليس لديك مشكلة تتعلق بالبرامج الضارة، بل لديك مشكلة تتعلق بالخصم".
لقد كنا روادًا لمفهوم الأمن السيبراني الذي يركز على الخصم لأنه أفضل طريقة لحماية العملاء ووقف الخروقات. نحن نعرف
الخصم بشكل أفضل من أي شخص آخر، ونستخدم هذه الرؤية لتوجيه ابتكاراتنا وحماية العملاء ووقف الخروقات وزيادة
التكلفة على الخصم.

يتطلب المستقبل الآمن أساسًا قويًا. وهذا ما نقدمه من خلال منصة CrowdStrike Falcon® XDR التي تعتمد على الذكاء
الاصطناعي.
نحن نقود التقارب بين البيانات والأمن السيبراني وتكنولوجيا المعلومات، مع الذكاء الاصطناعي التوليدي وأتمتة سير العمل
المبنية بشكل أصلي داخل منصة موحدة واحدة لنمنحك أنت وفريقك السرعة التي تحتاجها

تغلب على الخصم.

آمل أن تجد تقرير التهديدات العالمية لعام 2024 من CrowdStrike مفيدًا وملهمًا في معركتنا المشتركة ضد الخصم. ستظل
CrowdStrike ثابتة في مهمتها لتقديم النتيجة الأمنية التي تحتاج إليها بشدة: إيقاف الاختراق.

George Kurtz

جورج كورتز

الرئيس التنفيذي/المؤسس المشارك لشركة CrowdStrike

جدول محتويات



مقدمة

بينما نتأمل مشهد التهديدات السيبرانية في عام 2023، يسود موضوع التخفي.

لقد واجه الخصوم سطح هجوم معزز بفضل التقدم في تكنولوجيا الدفاع عن التهديدات والوعي بالتهديدات، وقد استجابوا من خلال تبني واعتماد تقنيات تمكنهم من التحرك بشكل أسرع والتهرب

كشف.

وتتجلى هذه التقنيات بوضوح في الانتشار المستمر للجرائم الإلكترونية، وهي مشروع تجاري جذاب ومربح للغاية بالنسبة للعديد من المجرمين. ومن غير المستغرب أن تظل الجرائم الإلكترونية تشكل التهديد الأكثر انتشارًا في مشهد التهديدات في عام 2023، حيث استغل الخصوم التقنيات لتحقيق أقصى قدر من التخفي والسرعة والتأثير.

» تستمر عمليات الابتزاز وسرقة البيانات أن تكون جذابًا -وفي كثير من الأحيان أسهل -طريق تحقيق الربح، كما هو الحال كما يتضح من الزيادة بنسبة ٪76في عدد الضحايا المذكورين في مواقع التسرب المخصصة لشركة BGH

في حين تظل برامج الفدية هي الأداة المفضلة للعديد من الصيادين الكبار (BGH)لا يزال ابتزاز سرقة البيانات يمثل وسيلة جذابة -وغالبًا ما تكون -أصبح الطريق إلى تحقيق الربح أسهل، كما يتضح من الزيادة بنسبة 76%في عدد الضحايا الذين تم ذكر أسمائهم في مواقع التسريب المخصصة لـ BGH (DLSs)بين عامي 2022و3202.

واصل وسطاء الوصول تحقيق الربح من خلال توفير الوصول الأولي إلى تهديدات الجرائم الإلكترونية الممثلون على مدار العام، مع زيادة عدد مرات الدخول المعلن عنها بنسبة 20%اعتبارًا من عام 2022.

كما كان خصوم الدولة القومية نشطين طوال عام 2023وواصل الخصوم المرتبطون بالصين العمل بوتيرة لا مثيل لها في جميع أنحاء المشهد العالمي، مستغلين التخفي والحجم لجمع بيانات مراقبة المجموعات المستهدفة والاستخبارات الاستراتيجية والملكية الفكرية.

وفي مناطق أخرى من العالم، استمر الصراع في دفع نشاط الدول القومية والقراصنة الإلكترونيين. ففي عام 2023، ومع دخول الحرب بين روسيا وأوكرانيا عامها الثاني، حافظت مجموعات الخصوم والأنشطة المرتبطة بروسيا على مستويات عالية ومستدامة من النشاط لدعم جمع المعلومات الاستخباراتية من جانب جهاز الاستخبارات الروسي، والأنشطة التخريبية، والعمليات المعلوماتية التي تستهدف أوكرانيا ودول حلف شمال الأطلسي.



كما تم رصد خصوم مرتبطين بإيران وخصوم متسللين في الشرق الأوسط

إعادة توجيه العمليات السيبرانية في النصف الأخير من العام بما يتماشى مع العمليات الحركية الناجمة عن الصراع بين إسرائيل وحماس في عام 2023.

حافظ خصوم كوريا الشمالية على وتيرة عالية باستمرار طوال عام 2023.
واستمر نشاطهم في التركيز على المكاسب المالية عبر سرقة العملات المشفرة وجمع المعلومات الاستخباراتية من المنظمات الكورية الجنوبية والغربية، وخاصة في القطاعات الأكاديمية والفضاء والدفاع والحكومة والتصنيع والإعلام والتكنولوجيا.

وفي مختلف أنحاء العالم، لعبت عمليات التخفي دوراً رئيسياً في أنشطة الخصوم التي تركز على المراقبة الرقمية وجمع المعلومات والسيطرة عليها دعماً لأجندات الحكومات. واستمر النطاق الجغرافي المقدر لهذا النشاط، فضلاً عن قدرات الجهات الفاعلة في التهديد العالمي ونطاق استهدافها، في التأكيد على مدى انتشار قدرات التطفل المستهدفة إلى ما هو أبعد من تلك التي أظهرتها البلدان التي يتم الإبلاغ عنها عادة. وفي بعض الحالات، ساعدت جهات هجومية من القطاع الخاص وأطر محاكاة الخصوم المتاحة علناً في هذا النشاط.

إن أحد أهم الدوافع التي تدفع الجهات الفاعلة إلى التخفي في عمليات التهديد السيبراني هو تطوير CrowdStrikeلمنتجات وشراكات جديدة طوال عام 2023. وقد غيرت هذه المنتجات والشراكات المخاطر داخل المشهد التشغيلي ولم تترك للخصوم مكانًا للاختباء.

في عام 2023اندمجت شركتا CrowdStrike® Falcon OverWatch™ وCrowdStrike Falcon® Intelligence لتصبحا شركة Adversary Operations (CAO). من خلال الجمع بين قوة استخبارات التهديدات وسرعة فرق الصيد المتخصصة وتريليونات أحداث القياس عن بعد المتطورة من منصة CrowdStrike Falcon® التي تعمل بالذكاء الاصطناعي والتي تكتشف وتعطل وتوقف خصوم اليوم المتطورين، أدى هذا الاندماج إلى زيادة تكلفة الأعمال المترتبة على إجراء الهجمات الإلكترونية بشكل كبير.

في عام 2024، قامت CrowdStrike CAO بإعادة تعبئة وحدات استخبارات التهديدات الخاصة بـ CrowdStrike إضافة خاصية البحث عن التهديدات المُدارة (الأولى من نوعها في الصناعة)، مما يمكّن المؤسسات من ملاحقة الخصوم ووقف الخروقات بشكل أفضل.

على مدار عام 2023، قدمت CrowdStrike CAO 34 خصمًا جديدًا -بما في ذلك خصم تم تعقبه حديثًا ومقره مصر، - WATCHFUL SPHINX مما رفع العدد الإجمالي للجهات الفاعلة التي تم تعقبها عبر جميع الدوافع إلى 232. بالإضافة إلى

من بين الخصوم المعروفين، يتتبع CrowdStrike CAO أكثر من 130 مجموعة من الأنشطة الخبيثة النشطة.

يقود CrowdStrike CAO تغطية تقاريرية لا مثيل لها وقابلة للتنفيذ تلتقط تطورات التهديدات السيبرانية الجديدة في الوقت الفعلي وتحدد الخصوم الجدد وتتعقبهم. يسلط تقرير التهديدات العالمية لعام 2024 من CrowdStrike الضوء على الاتجاهات البارزة من العام الماضي، وكيف تتطور أنشطة الخصوم ودوافعهم والطرق التي تتوقع بها CrowdStrike أن يتطور مشهد التهديدات

في العام القادم.

»

على مدار عام 2023،
تم تقديم لعبة CROWDSTRIKE CAO 34
أعداء جدد —بما في ذلك
مسار جديد تم تتبعه، ومقره مصر
الخصم، أبو الهول اليقظ —
رفع العدد الإجمالي
الممثلون الذين تم تتبعهم عبر جميع
الدوافع إلى 232.
بالإضافة إلى الاسم المذكور
الخصوم، حشد يضربون كاو
أكثر من 130 مسارًا نشطًا
مجموعات الأنشطة الخبيثة.



كراود سترايك
ابتكارات CAO

يقدم فريق CAOالتابع لـ CROWSTRIKEرؤى سريعة حول الأيدي
من فرق الخطوط الأمامية حتى يتمكنوا من تعطيل الخصوم بشكل أسرع
من أي وقت مضى.

في خريف عام 2023، طرحت شركة CROWSTRIKE CAOهوية جديدة
القدرة على تعقب التهديدات، وربط أحدث المعلومات الاستخباراتية
الدوافع والتكتيكات والأساليب والإجراءات المعادية (TTPS)
مع حماية الهوية من التهديدات من ELITEو CROWDSTRIKE FALCON®
يقوم صائدو التهديدات CAOبالتعرف بسرعة على التهديدات المخترقة ومعالجتها
الاعتمادات، وتتبع الحركة الجانبية والبقاء في المقدمة
الخصوم مع التغطية على مدار 24/7.

وبينما يبحث فريق CAOعن نشاط معادٍ في الداخل
منظمات العملاء، "سطح الهجوم الخارجي" الجديد
تتيح خاصية "الاستكشاف" للعملاء البحث والفحص
البنية التحتية للخصم.

قامت شركة CROWSTRIKEباستثمارات رئيسية في مجال الأتمتة في عام 2023، مما ساعد
يتخذ العملاء إجراءات فورية بشأن التهديدات التي تم تحديدها بواسطة CAO.عبر
تم تقديم FALCON IDENTITY THREAT PROTECTIONو CROWSTRIKEالجديد
عمليات سير العمل الآلية لإعادة تعيين كلمات مرور العملاء المعروضة على
THE CRIMINAL UNDERGROUND؛حظر النطاقات المنسوخة بنقرة واحدة
والإسقاط؛ ودليل اللعب الجديد لـ CROWSTRIKE FALCON® FUSION
للمؤشرات التلقائية للاختراق (IOCS)الناتجة عن
تهديدات التلاعب بالألفاظ وتكامل الأنظمة مع الجهات الخارجية.
تتيح التحسينات الجديدة للمستخدمين الاستجابة السريعة للتهديدات
في جميع مراحل سير عملهم الأمني.

وحدات CAOالجديدة من CROWDSTRIKE — CROWDSTRIKE FALCON® ADVERSARY
OVERWATCH™، CROWDSTRIKE FALCON®استخبارات الخصم و
جهاز كراودسترايك فالكون® أدفيرساري هانتر –لديه خاصية اصطياد التهديدات المرتبطة
أقرب إلى قدراتهم الاستخباراتية، مما يوحدهم
تجربة المستخدم حتى يتمكن العملاء من الاستفادة بسهولة من تطبيق واحد،
واجهة مستخدم متسقة لعرض المعلومات المهمة عبر جميع
قدرات CAO.

يستفيد عملاء CROWSTRIKEأيضًا من السياق المحسّن حول
الملاحظات، تكاملات مؤشر الهجوم الجديد (IOA)
تسريع إدارة المعلومات الأمنية والأحداث (SIEM)
الكشف والاستجابة، وتدفقات العمل الخاصة بمطاردة التهديدات التي من شأنها أن تساعد في زيادة
تحديد التهديدات البيئية والتحسينات بشكل فعال
لتوحيد البيانات وربطها عبر منصة فالكون
تطبيقات الطرف الثالث.

الدولة القومية أو الفئة	الخصم
روسيا	دُبٌ
فيتنام	بوفالو
جمهورية كوريا الديمقراطية الشعبية (كوريا الشمالية)	يخسر
جمهورية كوريا	رافعة
سوريا	الصقر
هاكتيفيست	ابن آوى
إيران	هريرة
باكستان	النمر
جورجيا	الوشق
كولومبيا	أوسيلوت
جمهورية الصين الشعبية	باندا
مصر	أبو الهول
جريمة	العنكبوت
الهند	نمر
ديك رومى	ذئب



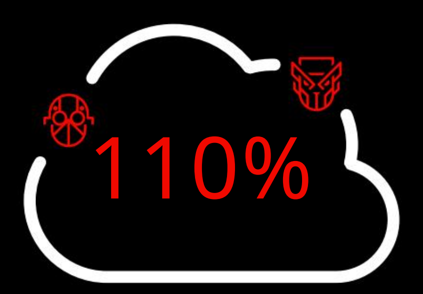
تهديد
منظر جمالي
ملخص

سنة بعد سنة (YoY) =



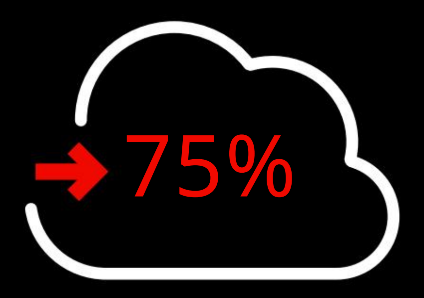
34عدوًا جديدًا تم تعقبهم بواسطة

CrowdStrike،مما رفع الإجمالي إلى 232



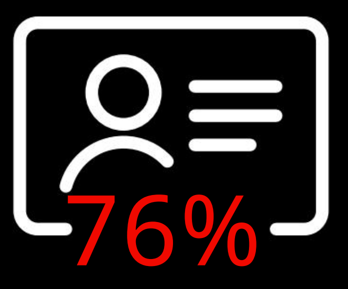
زيادة حالات الوعي السحابي

بنسبة 110%على أساس سنوي



تزايدت عمليات اختراق بيئة السحابة

بنسبة 75%على أساس سنوي



زيادة بنسبة 76%على أساس سنوي في عدد الضحايا المذكورين

مواقع مخصصة لتسريب المعلومات حول الجرائم الإلكترونية



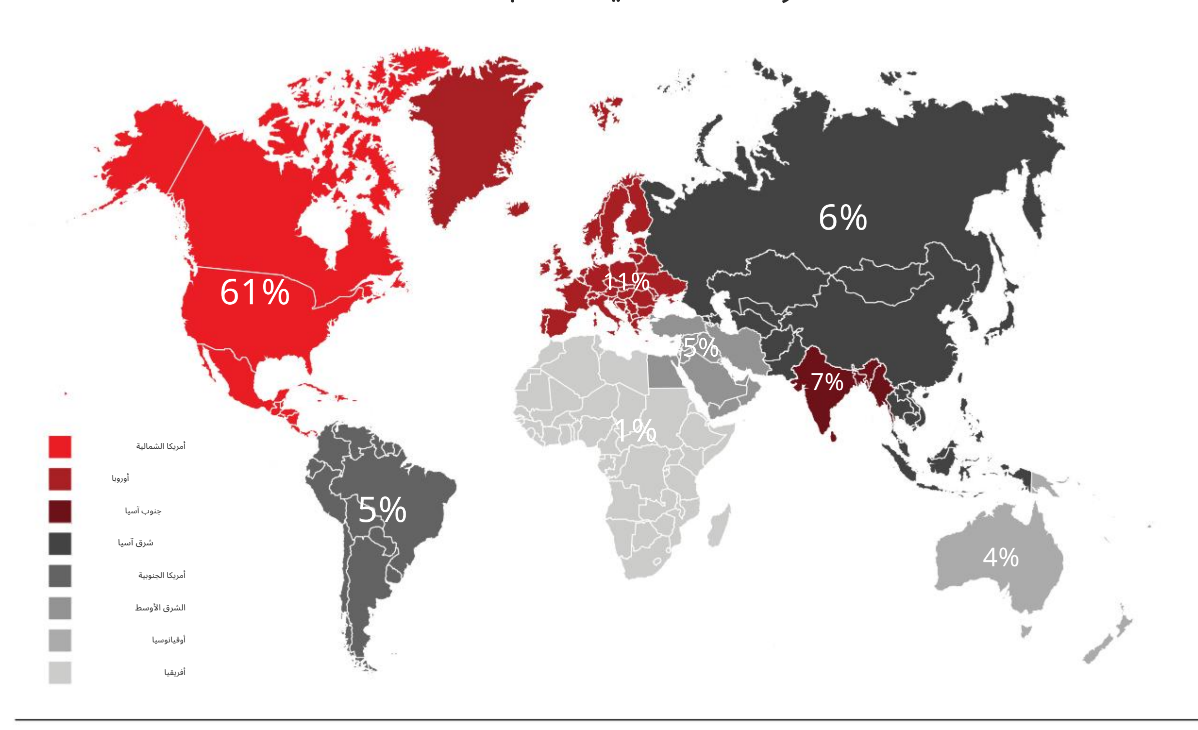
84%من عمليات الاختراق التي تنسب إلى الخصوم عبر السحابة كانت تركز على الجرائم الإلكترونية

إن التهديدات الإلكترونية اليوم مثيرة للقلق بشكل خاص بسبب الاستخدام الواسع النطاق لتقنيات "الاختراق التفاعلي"، والتي تنطوي على قيام الخصوم بتنفيذ إجراءات نشطة على المضيف لتحقيق أهدافهم. وعلى عكس هجمات البرامج الضارة التي تعتمد على نشر أدوات وبرامج نصية ضارة، فإن الاختراقات التفاعلية تستفيد من الإبداع ومهارات حل المشكلات لدى الخصوم من البشر. يمكن لهؤلاء الأفراد تقليد سلوك المستخدم والمسؤول المتوقع، مما يجعل من الصعب على المدافعين التمييز بين نشاط المستخدم المشروع والهجوم الإلكتروني.

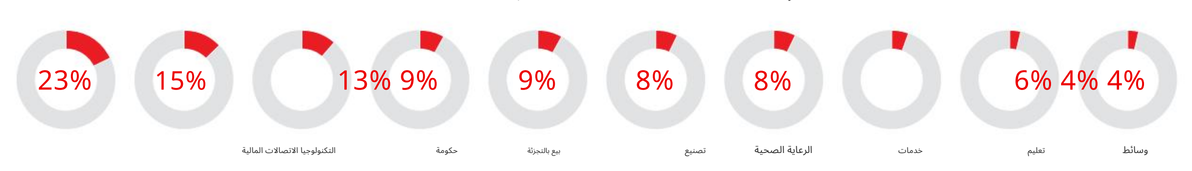
في عام 2023، لاحظت CrowdStrike زيادة بنسبة 60% على أساس سنوي في عدد حملات الاختراق التفاعلية، مع زيادة بنسبة 73% في النصف الثاني مقارنة بعام 2022.

كان قطاع التكنولوجيا هو القطاع الأكثر استهدافًا حيث لاحظت CrowdStrike CAO نشاط الاختراق التفاعلي في عام 2023، وهو اتجاه مستمر من عام 2022. تعكس المخططات أدناه التردد النسبي للاختراقات في أكبر 10 قطاعات صناعية وفي المناطق الجغرافية.

الاختراقات التفاعلية حسب المنطقة





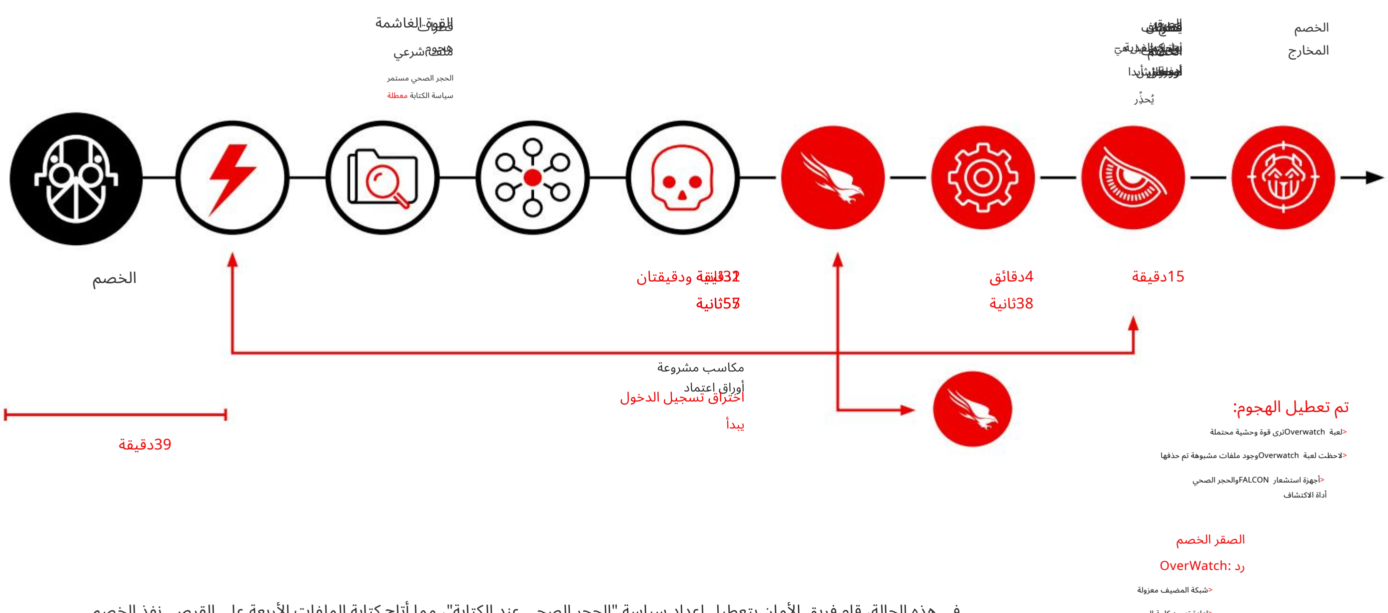


بعد الحصول على إمكانية الوصول الأولية إلى الشبكة، يسعى الخصوم إلى "الخروج" والانتقال أفقيًا من المضيف المخترق إلى مضيفين آخرين داخل البيئة. والوقت الذي يستغرقه الخصوم للقيام بذلك - "وقت الخروج" - أمر بالغ الأهمية لأن الأجهزة التي تم اختراقها في البداية نادرًا ما تكون هي الأجهزة التي يحتاجها الخصوم لتحقيق أهدافهم. يجب عليهم التحرك أفقيًا إلى الشبكة وإجراء الاستطلاع وإنشاء الثبات وتحديد أهدافهم. يتيح الاستجابة ضمن نافذة وقت الخروج للمدافعين التخفيف من التكاليف والأضرار الأخرى المرتبطة بالاختراقات.

انخفض متوسط وقت الهروب لنشاط اختراق الجرائم الإلكترونية التفاعلية هذا العام من 84 دقيقة في عام 2022 إلى 62 دقيقة في عام 2023. وكان أسرع وقت هرب تم رصده دقيقتين و7 ثوانٍ فقط.

تشريح الجريمة الإلكترونية
التطفل التفاعلي

للحصول على فهم أفضل للاختراقات التفاعلية، يوضح الجدول الزمني التالي سرعة الهجوم العملي في العالم الحقيقي:



في هذه الحالة، قام فريق الأمان بتعطيل إعداد سياسة "الحجر الصحي عند الكتابة"، مما أتاح كتابة الملفات الأربعة على القرص. نفذ الخصم أداة مشروعة للحصول على معلومات النظام للاستطلاع ثم أسقط ثلاثة ملفات أخرى، بما في ذلك برامج الفدية، على النظام.

حاولوا تنفيذ أداة اكتشاف واستطلاع الشبكة لرسم خيارات الحركة الجانبية، والتي تم حظرها على الفور وحجرها بواسطة مستشعر Falcon. تسبب هذا في قيام الخصم بفتح لوحة التحكم لفهم أداة الأمان المستخدمة. عندما حددوا منصة Falcon، لم يحاولوا أبدًا تنفيذ أداة الاكتشاف الثانية أو برنامج الفدية (الذي كان من الممكن منعه وحجره) ونقله إلى ضحية أخرى. في غضون دقائق، أخطر صائدو التهديدات العميلCrowdStrike CAO، وأوقفوا الجهاز عن العمل وأعادوا تعيين كلمة مرور المستخدم.

بمجرد حدوث اختراق أولي، لا يستغرق الأمر سوى ثوانٍ حتى يتمكن الخصوم من إسقاط أدوات و/أو برامج ضارة على بيئة الضحية أثناء الاختراق التفاعلي. ومع ذلك، فإن المثل القائل "الوقت من ذهب" ينطبق على الخصوم.

تم تخصيص أكثر من 88%من وقت الهجوم للاقتحام والحصول على الوصول الأولي. ومن خلال تقليل هذا الوقت أو القضاء عليه، يحرر الخصوم الموارد لشن المزيد من الهجمات.

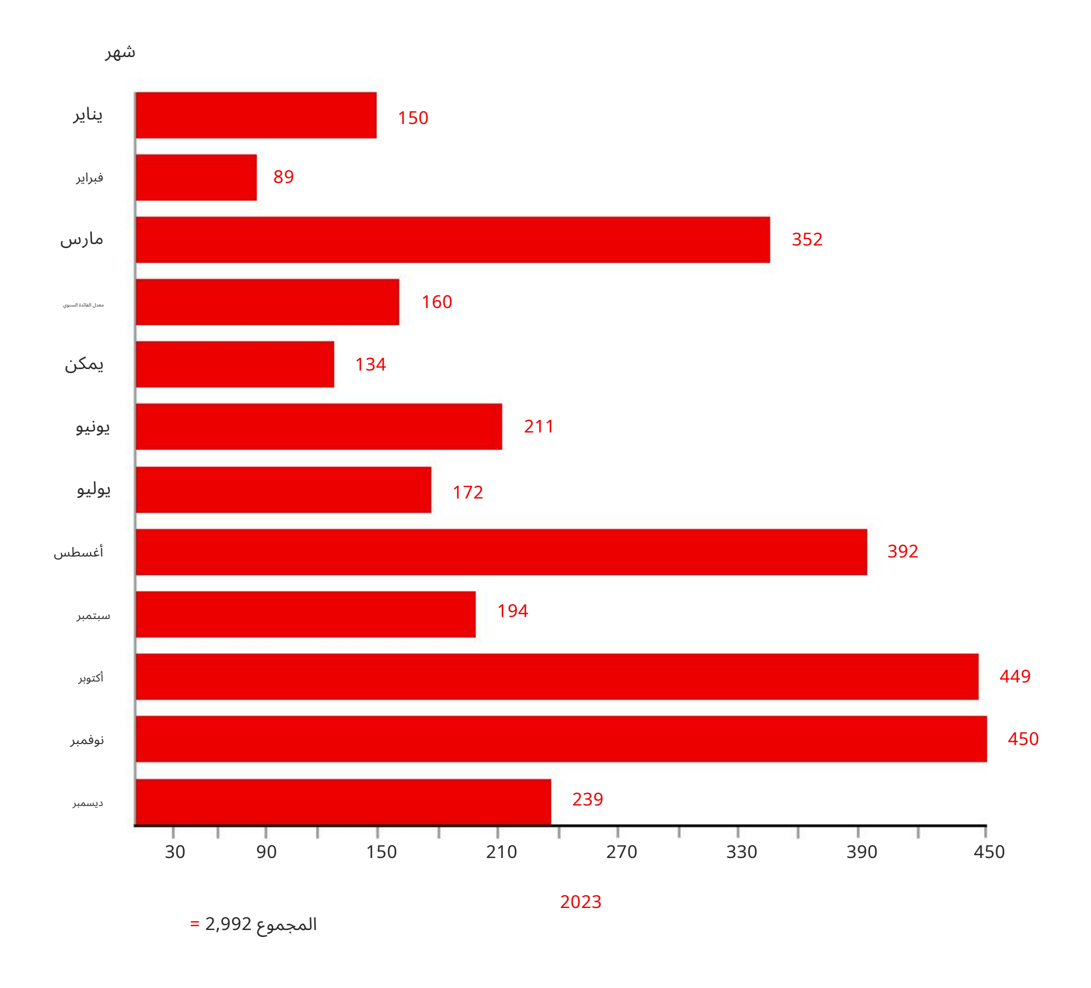
وللقيام بذلك، واصلوا الانتقال من البرامج الضارة إلى وسائل أسرع وأكثر فعالية مثل هجمات الهوية (التصيد الاحتيالي والهندسة الاجتماعية ووسطاء الوصول) واستغلال الثغرات والعلاقات الموثوقة. وهذا الاتجاه واضح على مدى السنوات الخمس الماضية، حيث مثل النشاط الخالي من البرامج الضارة 75%من حالات الاكتشاف في عام 2023 - ارتفاعًا من 71%في عام 2022.

خالية من البرامج الضارة

»

75% 2023
71% 2022
62% 2021
51% 2020
40% 2019

يرتبط هذا الاتجاه جزئيًا بنجاح هجمات الهوية ووسطاء الوصول والإساءة المفرطة لبيانات الاعتماد الصالحة لتسهيل الوصول والاستمرار في بيئات الضحايا. وسطاء الوصول هم جهات تهديد تكتسب حق الوصول إلى المنظمات وتوفر أو تبيع هذا الوصول إلى جهات فاعلة أخرى، بما في ذلك مشغلو برامج الفدية. استمر هؤلاء الخصوم في الاستفادة من توفير الوصول الأولي لمجموعة متنوعة من الجهات الفاعلة في تهديد الجرائم الإلكترونية في عام 2023، مع زيادة عدد عمليات الوصول المعلن عنها بنحو 20٪ مقارنة بعام 2022.



لا تستغرق الهجمات الإلكترونية المتطورة اليوم سوى بضع دقائق حتى تنجح. يستخدم الخصوم تقنيات مثل الهجمات التفاعلية باستخدام لوحة المفاتيح والأدوات المشروعة لمحاولة الاختباء من الاكتشاف. ولتسريع وتيرة الهجوم بشكل أكبر، يمكن للخصوم الوصول إلى بيانات الاعتماد بطرق متعددة، بما في ذلك شرائها من وسطاء الوصول مقابل بضع مئات من الدولارات. ويتعين على المنظمات إعطاء الأولوية لحماية الهويات في عام 2024.

2023
المواضيع

ة

هجمات الهندسة الاجتماعية

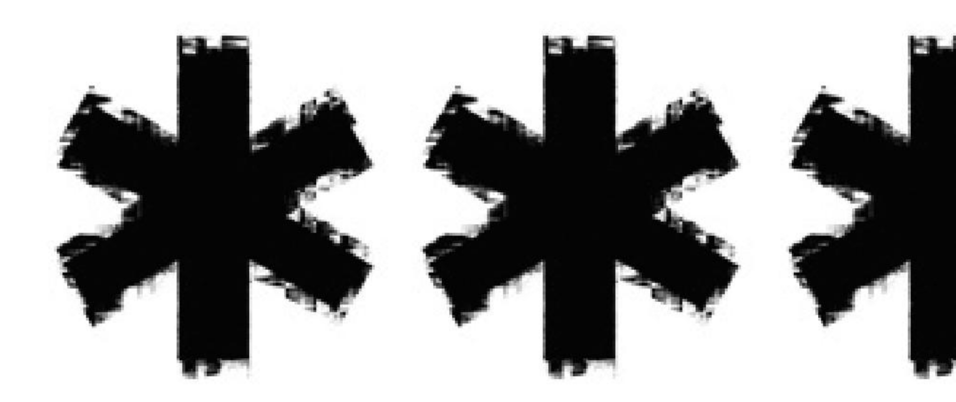
يواصل الخصوم من مختلف الدوافع والمناطق استخدام تقنيات التصيد الاحتيالي التي تنتحل هوية المستخدمين الشرعيين لاستهداف الحسابات الصالحة،

بالإضافة إلى بيانات المصادقة والتعريف الأخرى، لتنفيذ هجماتهم.

بالإضافة إلى سرقة بيانات اعتماد الحساب، لاحظ CrowdStrike CAO أن الخصوم يستهدفون مفاتيح وأسرار APIوملفات تعريف الارتباط والرموز الخاصة بالجلسة،

كلمات مرور لمرة واحدة (OTPs)وتذاكر Kerberosطوال عام .2023





بيانات اعتماد الحساب

يمكن للمهاجمين التحقق من صحة النظام و/أو حساب المستخدم باستخدام بيانات اعتماد مسروقة، والتي يمكن للمهاجم الحصول عليها إما بشكل مباشر (على سبيل المثال، باستخدام سارقي المعلومات أو استغلال أجهزة الحافة غير المدارة) أو عن طريق شرائها.

مفاتيح وأسرار API

قد يسمح الوصول إلى الموارد المحمية باستخدام مفاتيح وأسرار API المسروقة للخصم بسرقة بيانات حساسة. ما لم يتم تغيير مفاتيح وأسرار API، فقد يتمكن الخصم من الحفاظ على وصول غير محدد.

ملفات تعريف الارتباط والرموز الخاصة بالجلسة

يمكن للمهاجمين سرقة ملفات تعريف الارتباط والرموز الخاصة بالجلسة للتظاهر بأنهم المستخدم الشرعي والتحقق من صحة التطبيق.

كلمات المرور لمرة واحدة (OTPs)

تسمح سرقة OTP للخصم بتجاوز المصادقة متعددة العوامل (MFA) من خلال تبديل بطاقة SIM، أو هجمات SS7، أو الهندسة الاجتماعية للضحية، أو اختراق البريد الإلكتروني.

تذاكر كيربيروس و كيربيروس

من خلال سرقة أو تزوير تذاكر Kerberos، يمكن للمهاجمين الوصول إلى بيانات اعتماد مشفرة، والتي يمكن بعد ذلك اختراقها دون اتصال بالإنترنت. سجلت CrowdStrike CAO زيادة بنسبة 583% في هجمات Kerberosting في عام 2023.

الشكل 1. متجهات الهجوم القائمة على الهوية



أعداء الدب
اعتماد السلوك
حملات التحصيل

أجرت FANCY BEAR حملات منتظمة لجمع بيانات الاعتماد طوال عام 2023.

في مارس 2023، قامت شركة Microsoft بإصلاح ثغرة أمنية جديدة في Microsoft Outlook (CVE-2023-23397)، والتي استغلتها FANCY BEAR منذ مارس 2022 على الأقل لطلب جلسات مصادقة NT LAN Manager من الأهداف باستخدام رسائل بريد إلكتروني مخصصة للتصيد الاحتيالي. أفادت القيادة السيبرانية البولندية أن الخصم استخدم بيانات المصادقة هذه للاتصال بخوادم Exchange وتغيير أذونات صندوق بريد الحسابات عالية القيمة الإضافية من خلال بروتوكول خدمات الويب Exchange.[1]

كما أجرت FANCY BEAR حملات تصيد بيانات الاعتماد وقامت بتطوير مجموعة أدوات مخصصة لالتقاط بيانات الاعتماد من مستخدمي ukr.net. webmail وYahoo! Mail

قام الخصم بتوسيع مجموعة الأدوات هذه لاستخدام تقنية المتصفح داخل المتصفح في أبريل 2023 وأضاف قدرات اعتراض المصادقة الثنائية إلى مجموعة أدواته لجمع كلمات المرور لمرة واحدة (OTP) المرسلة إلى جهة اتصال المصادقة الثنائية (على سبيل المثال، رقم هاتف) المرتبطة بالحساب المستهدف.

لقد أجرت COZY BEAR حملات تصيد بيانات الاعتماد باستخدام رسائل Microsoft Teams لطلب رموز MFA لحسابات Microsoft 365 منذ أواخر مايو 2023 على الأقل. إذا قبل المستخدم طلب الرسالة الأولي، تحاول COZY BEAR هندسة الهدف اجتماعيًا من خلال الادعاء بأنه تم إجراء تغيير على إعدادات MFA الحالية الخاصة به والإشارة إلى أن رمز MFA مطلوب للتحقق.

لاحظت خدمات ®CrowdStrike أن COZY BEAR يتصل بحساب مخترق باستخدام Microsoft Entra ID (المعروف سابقًا باسم Azure Active Directory) قبل تسجيل جهاز جديد وتمكين تسجيل الدخول عبر الهاتف بدون كلمة مرور للمستخدم.

قام الخصم أيضًا بتصدير الشهادات التي تحتوي على مفاتيح خاصة وطلب تذكرة مصادقة KRBTGT لحساب مختلف باستخدام شهادة تم إصدارها بشكل شرعي.

---

1 https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/



العنكبوت المبعثر تجري عمليات متطورة حملات الهندسة الاجتماعية

تشكل التقنيات المبنية على الهوية أيضًا عنصرًا أساسيًا في تجارة .SCATERED SPIDER طوال عام 2023، أجرى هذا الخصم حملات هندسية اجتماعية متطورة للوصول إلى حسابات الضحايا. تضمنت تكتيكات SCATTERED SPIDER التصيد عبر الرسائل القصيرة (smishing) والتصيد الصوتي (vishing) لجمع بيانات الاعتماد والمكالمات الهاتفية التي تم إجراؤها إلى مكاتب مساعدة منظمة الضحية لإقناع موظفي الدعم بتوفير كلمات المرور و/أو إعادة تعيين المصادقة الثنائية للحسابات المستهدفة. في كثير من الحالات، استفاد SCATTERED SPIDER أيضًا من عمليات الاختراق السابقة في منظمات الاتصالات لمبادلة أرقام هواتف الموظفين المستهدفة، مما مكن الخصم من تلقي رسائل نصية قصيرة تحتوي على رموز .OTP

يختار SCATTERED SPIDER عمدًا أهداف حملة الهندسة الاجتماعية من الموظفين في فرق أمن المعلومات وغيرها من الفرق المرتبطة بتكنولوجيا المعلومات. ويرجع هذا على الأرجح إلى وصول الموظفين المباشر إلى أدوات الأمان بالإضافة إلى التطبيقات والوثائق التي قد تدعم الحركة الجانبية والمزيد من اختراق الحسابات. وفي أقلية من الحوادث، استهدف SCATTERED SPIDER حسابات تخص موظفين لديهم وصول مباشر إلى الموارد المالية للشركة.

بالإضافة إلى ذلك، غالبًا ما يقوم SCATTERED SPIDER بتكوين وكلاء سكنيين ليظهروا كما لو كانوا يقومون بتسجيل الدخول إلى حسابات الضحايا من نفس المنطقة الجغرافية التي يتواجد بها مالك الحساب الشرعي. وبذلك، أظهر الخصم فهمه لسياسات الأمان المتعلقة بالهوية في المؤسسات.

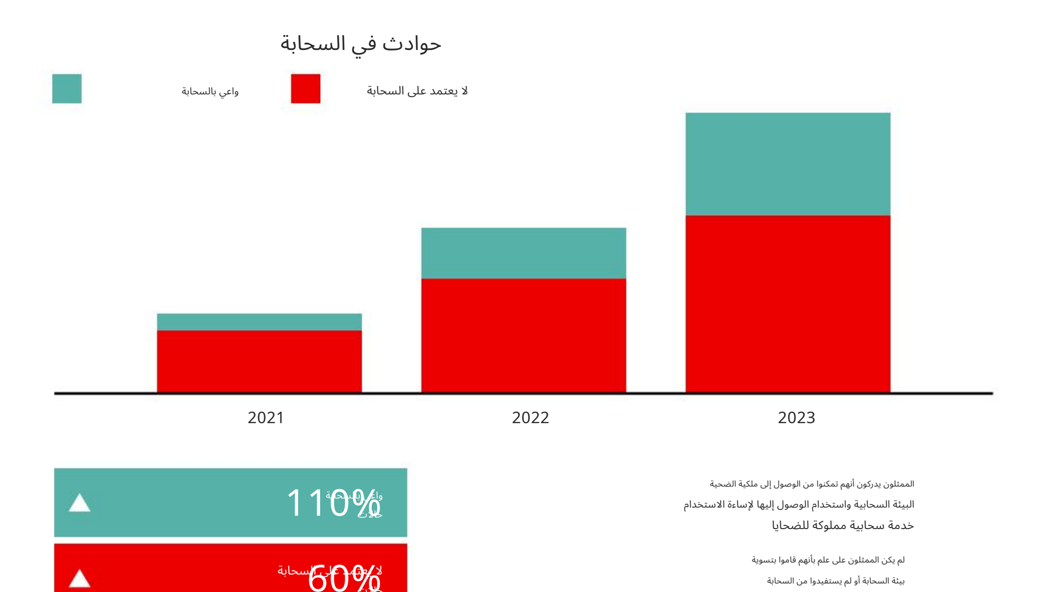


الخصوم مواصلة التطوير الوعي السحابي

كما كان متوقعًا، زادت حالات اختراق بيئة السحابة بنسبة 75% من عام 2022 إلى عام 2023 (الشكل 2)، مع زيادة الحالات المرتبطة بالسحابة بنسبة 110% وزيادة الحالات غير المرتبطة بالسحابة بنسبة 60%.

"الوعي السحابي" هو مصطلح يشير إلى الجهات الفاعلة المهددة التي تدرك قدرتها على اختراق أحمال العمل السحابية واستخدام هذه المعرفة لإساءة استخدام الميزات الفريدة للسحابة لأغراضها الخاصة.

ينشط مرتكبو الجرائم الإلكترونية بشكل خاص في استهداف البيئات السحابية: 84% من عمليات الاختراق التي تستهدف السحابة والتي تعزى إلى الخصوم تم تنفيذها من قبل الجهات الفاعلة المحتملة للجرائم الإلكترونية، مقارنة بـ 16% من الجرائم التي يتم تنفيذها عن طريق الاختراق المستهدف الجهات الفاعلة. أصبح خصوم BGH التقليديون، مثل INDRIK SPIDER، أكثر مواكبة للسحابة على مدار العام.



الشكل 2. الزيادة في حالات السحب

كان SCATTERED SPIDER هو المحرك الرئيسي لزيادة النشاط المرتبط بالسحابة طوال عام 2023، حيث كان مسؤولاً عن 29% من إجمالي الحالات. طوال عام 2023، أظهر SCATTERED SPIDER حرفية متقدمة ومتطورة

داخل بيئات السحابة المستهدفة للحفاظ على الاستمرارية والحصول على بيانات الاعتماد والتحرك أفقياً واستخراج البيانات.

إن تفضيل الخصوم للتقنيات القائمة على الهوية واضح في الهجمات التي تركز على السحابة. فيما يلي بعض الملاحظات حول الهجمات التي تركز على السحابة

الأنشطة التي تركز على الهوية والتي تم تصنيفها حسب مؤسسة MITRE ATT&CK® تكتيكات الوصول الأولي، والاستمرار، وتصعيد الامتيازات، والوصول إلى بيانات الاعتماد، والحركة الجانبية، والتسلل والتأثير.

»

كما هو متوقع، بيئة السحابة ارتفعت حالات الاختراق بنسبة 75% من عام 2022 إلى عام 2023 (الشكل 2). مع الحالات التي تتطلب الوعي السحابي زيادة بنسبة 110٪ والسحابة تزايد حالات اللاأدريين بنسبة 60%.





الوصول الأولي

اعتمد الخصوم على بيانات اعتماد صالحة لتحقيق الوصول الأولي.

لقد حصلوا على هذه بيانات الاعتماد من خلال تسريب بيانات الاعتماد عن طريق الخطأ، وهجمات القوة الغاشمة، والتصيد الاحتيالي/ الهندسة الاجتماعية، وسارقي بيانات الاعتماد، ووسطاء الوصول، وخدمات إعادة تعيين كلمة المرور الذاتية غير الآمنة، والتهديدات الداخلية.

في البرية

الدببة الفاخرة والعناكب المنتشرة تستهدف بشكل شائع Microsoft 365 بيانات الاعتماد عبر هجمات التصيد الاحتيالي.

المثابرة

للحفاظ على الوصول إلى Microsoft 365، وAzure حقق الخصوم عادةً الثبات على مستوى الهوية.

في البرية

إن تحقيق الاستمرارية على مستوى الهوية أمر شائع من خلال تسجيل عوامل المصادقة الإضافية في ENTRA ID.

استخدم SCATERED SPIDER مزود هوية لإنشاء الاستمرار في استخدام المجال الفيدرالي في معرف ENTRA، مبدئيًا الاعتماد على AADINTERNALS Azure AD BACKDOOR.2 تم توفير هذا الخصم ذو القدرة المستمرة على الوصول إلى معرفات الدخول المتعددة الهويات. في وقت لاحق، نقل العنكبوت المتناثر المفهوم إلى OKTA وإضافة مزود هوية اتحادي إلى حساب الضحية مستأجر أوكتا.

تصعيد الامتيازات

قام الخصوم بتصعيد الامتيازات من خلال الحصول على إمكانية الوصول إلى هويات إضافية

من بيانات الاعتماد المخزنة أو حملات الهندسة الاجتماعية أو بوابات إعادة تعيين كلمة المرور غير الآمنة. كما قاموا أيضًا بتصعيد الامتيازات عن طريق تعديل السياسات أو إضافة هويات إلى مجموعات أو أدوار مميزة.

في البرية

أثناء عملية اقتحام تستهدف برنامجًا في أمريكا الشمالية الشركة، العنكبوت المتناثر تصعيد الامتيازات عن طريق إرفاق سياسة وصول المسؤول الجديدة إلى مستخدم سحابي موجود مسبقًا، حيث أضافوا إليه مفتاح وصول جديد.

---

2 https://aadinternals.com/post/aadbackdoor/

الوصول إلى بيانات الاعتماد

قام الجهات الفاعلة في مجال التهديد بجمع بيانات الاعتماد من مخازن كلمات المرور و

مستودعات المعلومات.

في البرية

تم تخزين بيانات اعتماد INDRIK SPIDER المخزنة في .Azure Key Vault

في هجوم منفصل، تمكن العنكبوت المتفرق من الوصول إلى بيانات الاعتماد المخزنة في مدير الأسرار السحابي، وهو مدير أسرار قائم على الهوية

ونظام إدارة التشفير .SHAREPOINTو

في حالة أخرى، حدد العنكبوت المبعثر أيضًا نطاقًا

قام المتحكم الموجود داخل مستأجر Azureالخاص بالضحية بنسخ الأقراص

وأنشأوا آلة افتراضية جديدة يتم التحكم فيها بواسطة الخصم

حيث قاموا بتثبيت نسخ من أقراص وحدة التحكم بالمجال. من

تلك النسخ الموجودة على القرص، قام الخصم بإفراغ الدليل النشط (AD)

قاعدة البيانات .NTDS.DIT

الحركة الجانبية

انتقل الجناة من مكان إلى آخر بين المواقع المحلية و

البيئات السحابية.

في البرية

غالبًا ما يستخدم العنكبوت المتناثر الوصول إلى حسابات الضحايا على Microsoft 365

بيئات للبحث في SharePointعبر الإنترنت للخصوصية الافتراضية

تعليمات إعداد الشبكة (VPN)ثم تسجيل الدخول إلى VPN

وتم نقلها أفقيًا إلى الخوادم المحلية.

كما تم ملاحظة العنكبوت المبعثر باستخدام أوامر تشغيل Azureو

قدرات مماثلة للتحرك أفقيًا من التحكم السحابي

طائرة لحساب الحالات.

الترشيح

وقد قام الخصوم باستخراج البيانات باستخدام الأدوات، عن طريق تنزيل البيانات مباشرة من مستودعات يمكن الوصول إليها عبر الإنترنت -مثل SharePoint Onlineأو - GitHubأو عن طريق تحميل البيانات إلى خدمات الويب التي يمكن الوصول إليها عبر الإنترنت.

في البرية

استفادت SCATERED SPIDERمن متصفح S3مفتوح المصدر

استخراج البيانات إلى سحابة خارجية خاضعة لسيطرة الخصم

دلو التخزين.



تأثير

استهدف بعض الجهات الفاعلة في BGH المهتمين بالسحابة التخزين السحابي

كجزء من عملياتهم.

في البرية
لقد لاحظ كراود سترايك كاو على وجه التحديد عنكبوتًا متناثرًا يتبنى تكتيكات BGH ونشر برامج الفدية للتأثير. في حادثة منفصلة، قامت إحدى الشركات التابعة لشركة ALPHA SPIDER بنشر الأدوات التي تمكن Alphv من تشفير ملفات تخزين Azure الأسهم. في حادثة LockBit ، قام INDRIK SPIDER بحذف النسخ الاحتياطية مُخزَّنة في نسخ احتياطية .Azure لـ



استغلال العلاقات

طوال عام 2023، حاول مرتكبو الاختراق المستهدفون باستمرار

استغلال العلاقات الموثوقة للحصول على وصول أولي إلى المنظمات

عبر قطاعات ومناطق متعددة. يستغل هذا النوع من الهجمات

العلاقات بين البائع والعميل لنشر أدوات ضارة من خلال تقنيتين رئيسيتين: (1اختراق سلسلة توريد البرامج باستخدام مصادر موثوقة

(2استخدام البرمجيات الخبيثة لنشر الأدوات الخبيثة واستغلال الوصول إلى البائعين الذين يقدمون خدمات تكنولوجيا المعلومات.

إن الجهات الفاعلة المهددة التي تستهدف العلاقات مع أطراف ثالثة مدفوعة بـ

العائد المحتمل على الاستثمار (ROI): يمكن لمنظمة واحدة معرضة للخطر

تؤدي هذه الهجمات الخفية إلى مئات أو آلاف الأهداف اللاحقة. كما يمكن أن توفر هذه الهجمات الخفية فرصة أكثر فعالية للمهاجمين الذين يسعون

إلى استغلال هدف نهائي محصن.



تسليط الضوء على التهديد:

التنازلات في العلاقات القائمة على الثقة

الخصوم في الصين

في عام 2023، استهدف خصوم الصين بشكل متزايد العلاقات مع أطراف ثالثة في محاولة لنشر عمليات زرع ضارة والحصول على وصول أولي. استغل خصمان - CASCADE PANDA وJACKPOT PANDA -باستمرار شبكات موثوقة.

العلاقات من خلال اختراقات سلسلة التوريد والهجمات من قبل الجهات الفاعلة على الجانب أو الجهات الفاعلة في الوسط. في كل حالة، ركزت العمليات على
الضحايا الناطقون باللغة الصينية، مما قد يشير إلى وجود مراقبة محلية مستمرة.

طوال عام 2023، استمر JACKPOT PANDAفي استخدام الملفات القابلة للتنفيذ المصابة بأحصنة طروادة لنشر أدوات مساعدة ضارة أو عمليات زرع في المرحلة الثانية. بدءًا من مايو 2023، استخدم الخصم برنامج تثبيت مصاب بأحصنة طروادة لـ CloudChat، وهو تطبيق دردشة مقره الصين يحظى بشعبية لدى مجتمعات المقامرة غير القانونية الناطقة بالصينية في البر الرئيسي للصين. احتوى برنامج التثبيت المصاب بأحصنة طروادة الذي تم تقديمه من موقع CloudChatعلى المرحلة الأولى من عملية متعددة الخطوات والتي نشرت في النهاية - XShadeوهي عملية زرع جديدة مع كود يتداخل مع **عملية زرع** CplRATالفريدة لـ JACKPOT PANDA .

تم تحديد نشاط إضافي لـ JACKPOT PANDAفي مايو 2023 باستخدام أداة تنزيل .TEN موقعة، تسمى QuestDownloader، تم إطلاقها بواسطة عملية LiveHelp100.
يرتبط LiveHelp100بـ Comm100، وهي أداة مساعدة للبرمجيات استهدفتها عملية اختراق سلسلة توريد JACKPOT PANDAفي سبتمبر 2022. **تم استخدام** QuestDownloaderفي النهاية لنشر Cobalt Strikeو UltraVNC.

بدءًا من أواخر عام 2023، استخدمت CASCADE PANDAبشكل روتيني هجمات محتملة من قبل جهات وسيطة أو جهات جانبية لاعتراض حركة تحديث مشروعة من المرافق العامة، بالإضافة إلى أدوات باللغة الصينية، لنشر - WinDealerأداة الوصول عن بعد الضارة (RAT)المرتبطة بشكل فريد بهذا الخصم. في جميع حالات CASCADE PANDAمن هذه الفترة الزمنية، كانت عمليات تحديث البرامج المشروعة متصلة بالبنية الأساسية المشروعة المرتبطة بالمنتجات المعنية والبنية الأساسية المشروعة لمزود خدمة الإنترنت الصيني.

من المحتمل أن يقوم CASCADE PANDAبتوزيع WinDealerباستخدام البنية الأساسية المحلية لإعادة توجيه حركة المرور المشروعة أثناء النقل. في إحدى الحالات، استخدم CASCADE PANDAأداة ترجمة مشروعة باللغة الصينية مصابة بأحصنة طروادة لنشر WinDealer.

لمزيد من المعلومات حول أي من
الخصوم المذكورون في
هذا التقرير وتلك التي تستهدف
صناعتك أو منطقتك،
تحقق من CROWSTRIKE
الكون الخصم.



كما استغلت جهات تسلل مستهدفة غير منسوبة تستخدم التكتيكات والأساليب والتقنيات والأساليب المتسقة مع الخصوم المرتبطين بالصين العلاقات الموثوقة لإجراء عمليات في عام 2023.

على مدار النصف الثاني من العام، قام أحد الفاعلين غير المعروفين باختراق شركة برمجيات أمن المعلومات في الهند واستخدم الوصول الناتج عن ذلك لتوزيع ملفات قابلة للتنفيذ مصابة بأحصنة طروادة عبر عمليات تحديث البرامج المشروعة.

تستهدف هذه الهجمات ضحايا من مناطق وصناعات متعددة، بما في ذلك قطاعات البناء والخدمات المالية والحكومة والتكنولوجيا والاتصالات والخدمات اللوجستية في جميع أنحاء الولايات المتحدة والهند والبرازيل وسريلانكا والفلبين وزامبيا والمكسيك وماليزيا. ورغم أن نشاط استغلال العلاقات الموثوقة هذا لا يزال غير منسوب إلى جهة معينة، فإن الحمولة النهائية المستخدمة في هذا الهجوم تشترك في تداخلات كبيرة في التعليمات البرمجية مع BackShellو StealthPipes، وهما أداتان منسوبتان بشكل فريد إلى .WET PANDA

تم رصد جهة ثانية غير معروفة في أواخر عام 2023تقوم بتوزيع ShadowPadعلى أهداف مشتبه بها تتحدث اللغة الصينية كجزء من اختراق محتمل لسلسلة التوريد.

قام الفاعل باختراق منصة مؤتمرات افتراضية مقرها الصين واستغل الوصول الناتج عن ذلك لنشر مثبت ShadowPadملوثًا **بأحصنة طروادة** متنكرًا في هيئة أداة برمجية شرعية.

وعلى الرغم من عدم نسب هذا النشاط إلى جهة معينة، فإن ShadowPadيستخدم حصريًا من قبل خصوم مرتبطين بالصين مثل .VAPOR PANDAو WICKED PANDAو PANDA AQUATIC

في أوائل عام 2023، من المرجح أن يقوم أحد الجهات الفاعلة غير المنسوبة باختراق خادم تحديث مرتبط ببرنامج إدارة i4Toolsالخاص بـ iPhone لنشر AvanteGarde، وهو إطار عمل للبرامج الضارة مرتبط بمجموعة أنشطة InnateSparkالمرتبطة بالصين.

على الرغم من أن CrowdStrike CAOكان قادرًا على تأكيد اتصال 250عميلًا على الأقل بخادم التحديث المخترق، إلا أن 10%فقط تلقوا التحديث الخبيث، مما يشير على الأرجح إلى أن الفاعل قام باختيار أهداف عالية القيمة.

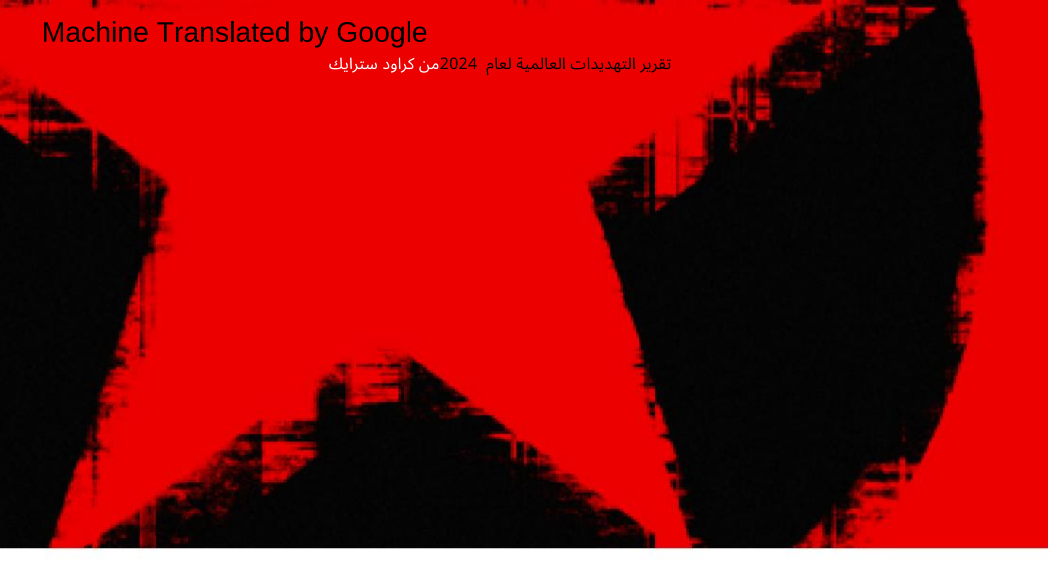
تسليط الضوء على التهديد:

سلسلة التوريد في كوريا الشمالية التسويات

كما أظهر خصوم جمهورية كوريا الشعبية الديمقراطية اهتمامًا متزايدًا باستغلال العلاقات القائمة على الثقة في عام 2023. وعلى وجه الخصوص، أساءت LABYRINTH CHOLLIMA استخدام علاقة موثوقة بين بائع تكنولوجيا وعميل في ثلاث حالات العام الماضي، مما يسلط الضوء على الاهتمام باستخدام اختراقات سلسلة التوريد كناقل للاختراق.

تم رصد هذا النوع من الاستغلال لأول مرة في مارس 2023، عندما قام أحد الخصوم باختراق برنامج لدى مزود VoIP 3CX. ويبدو أن هذا الاختراق بدأ باختراق سلسلة التوريد الأولية لشركة Trading Technologiesللتكنولوجيا المالية. استخدم الخصم إصدارات سطح المكتب 3CX Electron التي تحتوي على أحصنة طروادة لتوصيل سارقي المعلومات إلى بيئات الضحايا. ثم استمر الجناة في حملة يوليو 2023التي أساءت بشكل مماثل الوصول إلى شركة تكنولوجيا في محاولة لاختراق منتجها واستخدام البنية التحتية المشروعة للتسلل إلى البيئات المخترقة.

عملاء الشركة.



كما لاحظ CrowdStrike CAO أيضًا أن LABYRINTH CHOLLIMA يوزع البرامج الضارة من خلال متغير مشغل الوسائط CyberLink المزود بحصان طروادة. تبرز هذه الحملة بين عمليات اختراق أخرى لسلسلة توريد CHOLLIMA، LABYRINTH حيث استخدم الخصم حواجز تنفيذية تحد من الحملة إلى منطقة جغرافية محددة ونافذة زمنية، مما يشير إلى استهداف مجموعة معينة من الضحايا.

لا يزال الدافع وراء هذه الاختراقات غير محدد. في إحدى عمليات اختراق سلسلة التوريد، اكتشف CrowdStrike CAO برامج مصابة بأحصنة طروادة في بيئات 62 عميلاً؛ ومع ذلك، كانت عمليات اختراق سلسلة التوريد اللاحقة أكثر محدودية في نطاقها. ربما يستخدم الخصم عمليات اختراق سلسلة التوريد لإلقاء شبكة واسعة وتقديم أدوات متابعة مناسبة لأهداف مثيرة للاهتمام.

من المرجح أيضًا أن تستغل LABYRINTH CHOLLIMA العلاقات الموثوقة بين الموردين ومستخدمي المنتجات للتسلل إلى أهداف محددة عالية القيمة لتوليد العملات وحملات التجسس. يقدر CrowdStrike CAO أن المزيد من عمليات اختراق سلسلة التوريد الخاصة بـ CHOLLIMA LABYRINTH من المرجح أن تحدث في المستقبل القريب. من المرجح أن يعتبر الخصم اختراق سلسلة التوريد تكتيكًا مفيدًا مع إمكانية تبسيط العمليات. تم إجراء هذا التقييم

مع ثقة معتدلة استنادًا إلى حجم التنازلات في سلسلة التوريد

تمت ملاحظته في عام 2023.

التوقعات:

استغلال العلاقات مع أطراف ثالثة

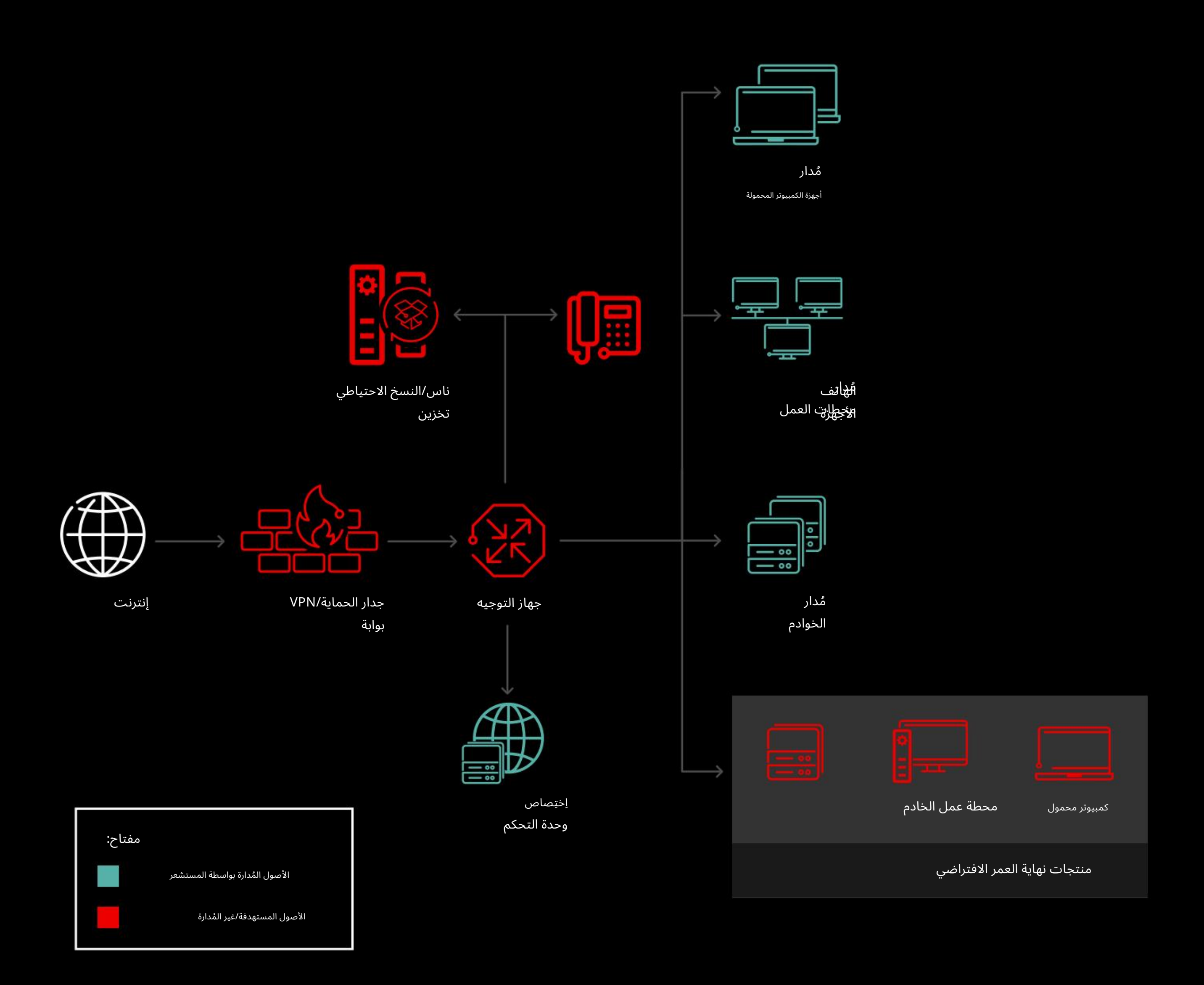
ستستمر عمليات اختراق العلاقات القائمة على الثقة في جذب الجهات الفاعلة المتطفلة المستهدفة في المستقبل القريب.
ومن المرجح أن يكون العائد المرتفع على الاستثمار في هذه الهجمات، وخاصة فيما يتعلق بالقدرة على الوصول إلى الاختراقات المحتملة في مجرى النهر مقارنة بالجهد المحدود المطلوب لاختراق هدف واحد، حافزًا لشن هجمات طوال عام 2024.

تتعرض المنظمات العاملة في قطاع التكنولوجيا لمخاطر فريدة من نوعها بسبب استغلال العلاقات مع أطراف ثالثة.
في عام 2023، نشأت كل حالات اختراق العلاقات الموثوقة تقريبًا كجزء من عملية اختراق في منظمة تابعة لقطاع التكنولوجيا تقدم برامج تجارية.

عف:

استغلال "تحت الرادار"

لقد تكيفت الجهات الفاعلة في مجال التهديدات مع الرؤية المحسنة لأجهزة استشعار الكشف والاستجابة التقليدية لنقاط النهاية من خلال تغيير تكتيكات الاستغلال الخاصة بها للوصول الأولي والحركة الجانبية. وهي تستهدف الآن محيط الشبكة، حيث تقل رؤية المدافعين بسبب احتمالية افتقار نقاط النهاية إلى أجهزة استشعار الكشف والاستجابة أو عدم قدرتها على دعم نشر المستشعرات (الشكل 3).



الشكل 3. الأهداف غير المُدارة على شبكة عامة

الأجهزة الشبكية غير المُدارة —وخاصة أجهزة البوابة الطرفية —

ظلت أكثر ناقلات الوصول الأولية التي يتم ملاحظتها بشكل روتيني للاستغلال خلال عام 2023. تعتمد هذه الأجهزة عادةً على بنية قديمة، مما يؤدي إلى استغلال نقاط الضعف على نطاق واسع في جدران الحماية ومنصات VPN من Citrix (CVE-2023-3519، CVE-2023-4966) و(CVE-2023-20198) Cisco و(CVE-2023-46747). 5F

» الأجهزة الشبكية غير المُدارة — بوابة الحافة بشكل خاص الأجهزة -ظلت الأكثر الملاحظة الأولية بشكل روتيني ناقل الوصول للاستغلال خلال عام 2023.

كما تم ملاحظة الاستغلال في العديد من الأجهزة الأخرى غير المُدارة طوال عام 2023. ومن المرجح أن يكون الجهات الفاعلة المستهدفة منخرطة في استهداف تطبيق إدارة الأجهزة المحمولة Ivanti الانتهازي عبر CVE-2023-35082 وCVE-2023-35078.

استغل مشغلو برنامج الفدية Akira ثغرات CVE-2023-27532 — وهي ثغرة أمنية في Veeam Backup & Replication — للتسلل إلى البنية الأساسية لتخزين النسخ الاحتياطية للضحية. بالإضافة إلى ذلك، طور مرتكبو الجرائم الإلكترونية ثغرات أمنية غير مرئية

منتجات هاتفية مبنية على مشروع مفتوح المصدر مهجور.

تتعلق الثغرة الأمنية الأخيرة بتوجه آخر لوحظ في عام 2023: التركيز على استغلال المنتجات التي انتهت صلاحيتها. حيث يعمل الجهات الفاعلة في مجال التهديد بنشاط على تطوير ثغرات أمنية لمنتجات انتهت صلاحيتها والتي لا يمكن تصحيحها وغالبًا لا تسمح بنشر أجهزة الاستشعار الحديثة. توفر خوادم أنظمة التشغيل غير المدعومة وأجهزة البوابة القديمة إمكانية الوصول بسهولة -حتى إلى عائلات البرامج الضارة القديمة -مما يؤدي إلى إصابات مستمرة تشتت الموارد عن قضايا الأمن المعاصرة.

» الجهات الفاعلة المهددة نشطة تطوير الثغرات من أجل نهاية العمر الافتراضي المنتجات التي لا يمكن تصحيحها وفي كثير من الأحيان لا تسمح بذلك نشر أجهزة الاستشعار الحديثة.

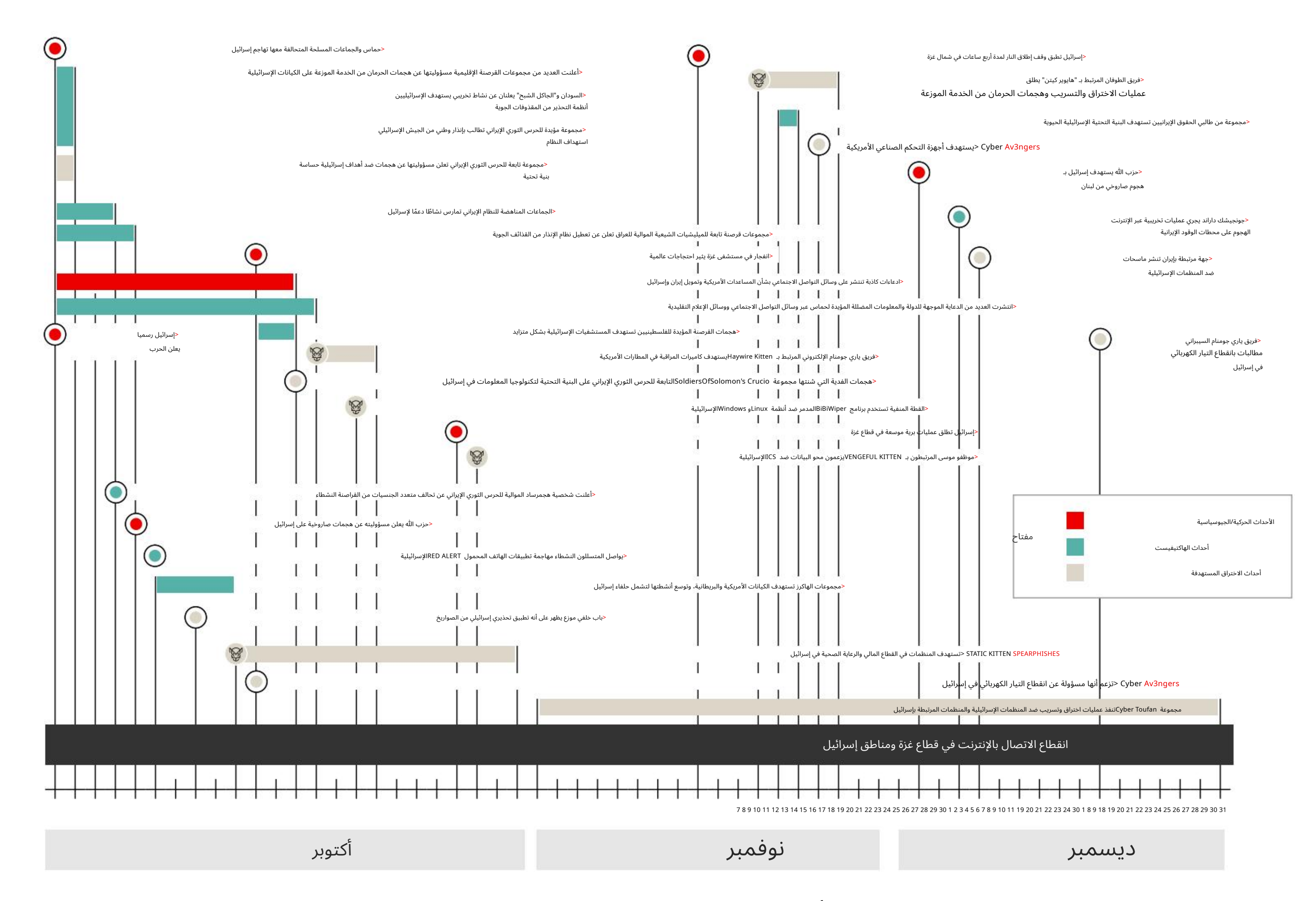
إن زيادة قدرة المدافعين على رؤية مثل هذه المتجهات الاستغلالية أمر أساسي في التخفيف من المخاطر التي تفرضها هذه التكتيكات. يمكن الاستفادة من CrowdStrike® Falcon Surface℠ لمراقبة وتقليل الخدمات المعرضة للإنترنت والحفاظ على مخزون التطبيقات عبر سطح الهجوم الخاص بالمؤسسة. يجب على المدافعين إعطاء الأولوية لتصحيح المنتجات المعرضة للخطر، وخاصة المنصات مفتوحة المصدر، عندما تكون المنتجات عرضة لثغرات معروفة في تنفيذ التعليمات البرمجية عن بُعد (RCE). أخيرًا، CrowdStrike Falcon®

يمكن لـ Spotlight تحديد ما إذا كانت الأصول التي تم نشرها بواسطة المستشعرات عرضة لثغرات أمنية معروفة ومتى وصلت هذه النقاط النهائية إلى نهاية عمرها الافتراضي.

الصراع بين إسرائيل وحماس 2023: العمليات السيبرانية تأثير

في السابع من أكتوبر 2023، شن الجناح العسكري لحركة حماس، كتائب عز الدين القسام، وعدة جماعات مسلحة أخرى مقرها غزة، هجومًا حركيًا ضخمًا ضد إسرائيل، مما أسفر عن مقتل مئات الإسرائيليين واحتجاز رهائن. في الأشهر التالية، تتبعت CrowdStrike CAO العمليات الإلكترونية الجارية من قبل جهات اختراق واختراق مستهدفة. تركز الأنشطة والمطالبات من كلتا المجموعتين في المقام الأول على استهداف التكنولوجيا التشغيلية أو الأنظمة الحرجة الأخرى -من المرجح أن تؤثر نفسياً على السكان المستهدفين -ونشر ماسحات مدمرة ضد الكيانات الإسرائيلية أو المرتبطة بإسرائيل.

تتضمن معظم العمليات السيبرانية المرتبطة بالصراع التي تم رصدها أنشطة قرصنة ناشطة وعمليات يقوم بها ناشطون مزيفون مشتبه بهم.
في سياق الصراع بين إسرائيل وحماس، أصبح الخط الفاصل بين هذين النوعين من الجهات الفاعلة المهددة غير واضح،
حيث تعمل مجموعات الهاكرز الحقيقية في كثير من الأحيان على تضخيم ادعاءات شخصيات غير أصلية من المحتمل أن تكون مرتبطة بالدولة أو تقديم الدعم لها.



الشكل 4. الأحداث الهامة المتعلقة بالصراعات السيبرانية والحركية

ركز الناشطون المزيفون المرتبطون بأعداء الدولة الإيرانية والناشطون الهاكرز الذين يطلقون على أنفسهم اسم "المؤيدون للفلسطينيين" على استهداف البنية التحتية الحيوية وأنظمة التحذير من المقذوفات الجوية الإسرائيلية والأنشطة المخصصة لأغراض العمليات المعلوماتية في عام 2023.

على الرغم من أن CrowdStrike CAO يتتبع العديد من الخصوم المرتبطين بجماعة حماس المسلحة، إلا أنه لم يتم ملاحظة أي نشاط منسوب إلى هؤلاء الخصوم فيما يتعلق بالصراع بين إسرائيل وحماس.

ومن المرجح أن يكون ذلك بسبب عدم توفر الموارد أو تدهور البنية التحتية للإنترنت وتوزيع الكهرباء في منطقة الصراع.

التظاهر

تم تقديم مصطلح "النشاط المزيف" في تقرير التهديدات العالمية لعام 2016 الصادر عن CROWSTRIKE، والذي يشير إلى إلى نشاط الكيانات التي تصف نفسها بأنها مجموعات من الناشطين الهاكرز ولكن من المرجح أن يمثلوا واجهة للحكومة أو أي جهة مهنية أخرى كيان.

في محاولة للظهور بمظهر حقيقي، يقوم المتطرفون المزيفون -أو الأشخاص غير الأصليين - غالبًا ما يتبنون الصور والبلاغة والتكتيكية والأسماء الموجودة الناشطون الهاكرز. غالبًا ما يظهرون كاستجابة مباشرة للتحديات الجيوسياسية الأحداث، غالبًا ما يكون لها تاريخ نشاط قليل أو لا يوجد تاريخ نشاط ثابت تقريبًا العمل دائمًا وفقًا لمصالح حكومة الولاية. توفر الشخصيات الداعمة للدولة طبقة من الإنكار ولكنها قد تخدم أيضًا أهداف عمليات المعلومات.



خصوم حماس
غائب بشكل ملحوظ عن
الأنشطة المتعلقة بالصراع

أظهرت مجموعة RENEGADE JACKAL، وEXTREME JACKAL التي من المرجح أن تكون من الخصوم المتمركزين في غزة، والتي تم تقييمها من قبل CrowdStrike، دعمها للمصالح الاستراتيجية لحماس.
بالإضافة إلى ذلك، تشير الأدلة إلى أن مجموعة أنشطة CruelAlchemy تمثل وحدة عمليات إلكترونية مرتبطة بحماس وموجودة فعليًا في تركيا.

كان RENEGADE JACKAL هو الخصم الأكثر نشاطًا في حماس طوال عام 2023. استهدفت المجموعة في المقام الأول الكيانات الحكومية في الشرق الأوسط ببرامجها الخبيثة المخصصة لنظام التشغيل Windows وزرع Android. في منتصف أكتوبر 2023، ربطت CAO RENEGADE JACKAL CrowdStrike بجيش القدس الإلكتروني، وهي مجموعة قرصنة ظاهرية أشار مسؤولون في حماس سابقًا إلى أنها تدعم

من وحدة الحرب السيبرانية IDQB.

وقد أشارت تقارير مفتوحة المصدر إلى وجود نشاط يُزعم أنه يُعزى إلى حماس، يستهدف أفراد قوات الدفاع الإسرائيلية. ومع ذلك، ليس لدى CAO CrowdStrike أي دليل آخر يشير إلى أن الخصوم المذكورين أعلاه يستهدفون حاليًا كيانات إسرائيلية فيما يتعلق بالأحداث الأخيرة في إسرائيل وغزة.[3]

منذ بداية الصراع، تدهورت الاتصالات عبر الإنترنت في قطاع غزة بشكل كبير بسبب مزيج من النشاط الحركي وانقطاع التيار الكهربائي وهجمات الحرمان من الخدمة الموزعة (DDoS).

من المرجح أن يكون انقطاع التيار الكهربائي والإنترنت قد أعاق عمليات العدو المتمركزة في غزة. ورغم عدم ملاحظة أي نشاط لـ CruelAlchemy مرتبط بشكل مباشر بالصراع بين إسرائيل وحماس، فقد تم تحديد مراكز القيادة والسيطرة

(C2) تشير البنية التحتية إلى أن الفاعل ظل نشطًا بعد ظهور الصراع، مما قد يدعم التقارير السابقة التي تشير إلى أن CruelAlchemy تعمل من خارج غزة.

عمليات القرصنة واسعة النطاق
نطاق طيف التحفيز
إظهار الاهتمام المشترك بالأنظمة الحرجة

ورغم أن اندلاع الصراع بين إسرائيل وحماس في السابع من أكتوبر/تشرين الأول 2023 أشعل موجة من أنشطة القرصنة الإلكترونية المؤيدة لفلسطين والمؤيدة لإسرائيل، فإن الأولى تفوقت كثيراً على الثانية. فقد أعلن قرصنة إلكترونية معروفون وغير معروفين من قبل داخل منطقة الصراع ومن مختلف أنحاء العالم عن مسؤوليتهم عن هذا النشاط، الذي دار جزء كبير منه حول محاولة أو مزعومة إنشاء نظام تحذير من المقذوفات الجوية وتعطيل البنية التحتية الحيوية التي تستهدف إسرائيل. كما قام عدد أقل من القرصنة الإلكترونية بتوسيع نطاق عملياتهم خارج منطقة الصراع لاستهداف الدول أو الكيانات التي تعتبر داعمة لإسرائيل.

---

3 https://www.timesofisrael.com/liveblog_entry/idf-exposes-catfishing-network-seeking-to-extract- معلومات من القوات التابعة لحماس

أنظمة تحذير المقذوفات الجوية واستهداف البنية التحتية الحيوية

استهدفت العديد من كيانات القرصنة أنظمة الإنذار بالقذائف الجوية في إسرائيل وزعمت أنها عطلت أنظمة الدفاع الصاروخي والمدفعية وقذائف الهاون التابعة لجيش الدفاع الإسرائيلي لمنع توصيل الإخطارات و/أو إرسال إشعارات كاذبة بهجوم وشيك إلى المواطنين الإسرائيليين. وقد انخفض استهداف هذه الخدمات بعد منتصف أكتوبر 2023؛ ومع ذلك، فإن زيادة النشاط الحركي في المنطقة قد تشعل اهتمامًا متجددًا بمزيد من التعطيل أو الإخطارات الكاذبة.

طوال مدة الصراع، استهدف نشطاء القرصنة المؤيدين لفلسطين باستمرار البنية التحتية الحيوية في إسرائيل، بما في ذلك الأنشطة التخريبية ضد البنية التحتية لتوزيع الطاقة ومضخات المياه، وهجمات الحرمان من الخدمة الموزعة ضد شركات المرافق، وعمليات القرصنة والتسريب ضد محطات معالجة المياه والطاقة. من المرجح أن يكون هذا النشاط محاولة لإلحاق الضرر الجسدي والنفسي بالمواطنين الإسرائيليين ومن المرجح أن يستمر طوال مدة الصراع بين إسرائيل وحماس. تم إجراء هذا التقييم بثقة عالية بناءً على الاستهداف المستمر حتى الآن والنشاط المماثل الذي لوحظ في صراعات أخرى حديثة.

مثل الحرب بين روسيا وأوكرانيا.

العمليات التي تتجاوز اللحظة منطقة الصراع

امتد نشاط القرصنة المحدود إلى ما هو أبعد من منطقة الصراع المباشرة ردًا على الدعم الحقيقي أو المتصور لإسرائيل. في 12 أكتوبر، 2023،

[illegible] في الولايات المتحدة، زاعمة أن

في 14 أكتوبر، 2023، أعلنت مجموعة قرصنة شهيرة في جنوب آسيا مسؤوليتها عن هجوم DDoS ضد موقع عسكري بريطاني. وكان هذا النشاط مصحوبًا بإشارات إلى دعم المملكة المتحدة لإسرائيل.

في يونيو 2023 باكستان

في 16 أكتوبر، 2023، من المحتمل أن تكون مجموعة قرصنة إندونيسية تطلق على نفسها اسم شاركوا بيانات مسربة، مدعيين أنهم انتهكوا البيانات الشخصية القابلة للتحديد معلومات شخصية (PII) عن ما يقرب من 790 ألف طبيب في الولايات المتحدة. ويقال إن التسريب المزعوم جاء انتقاما لدعم الولايات المتحدة لإسرائيل وكذلك لإظهار الدعم للفلسطينيين.

لإنهائه بصيرة

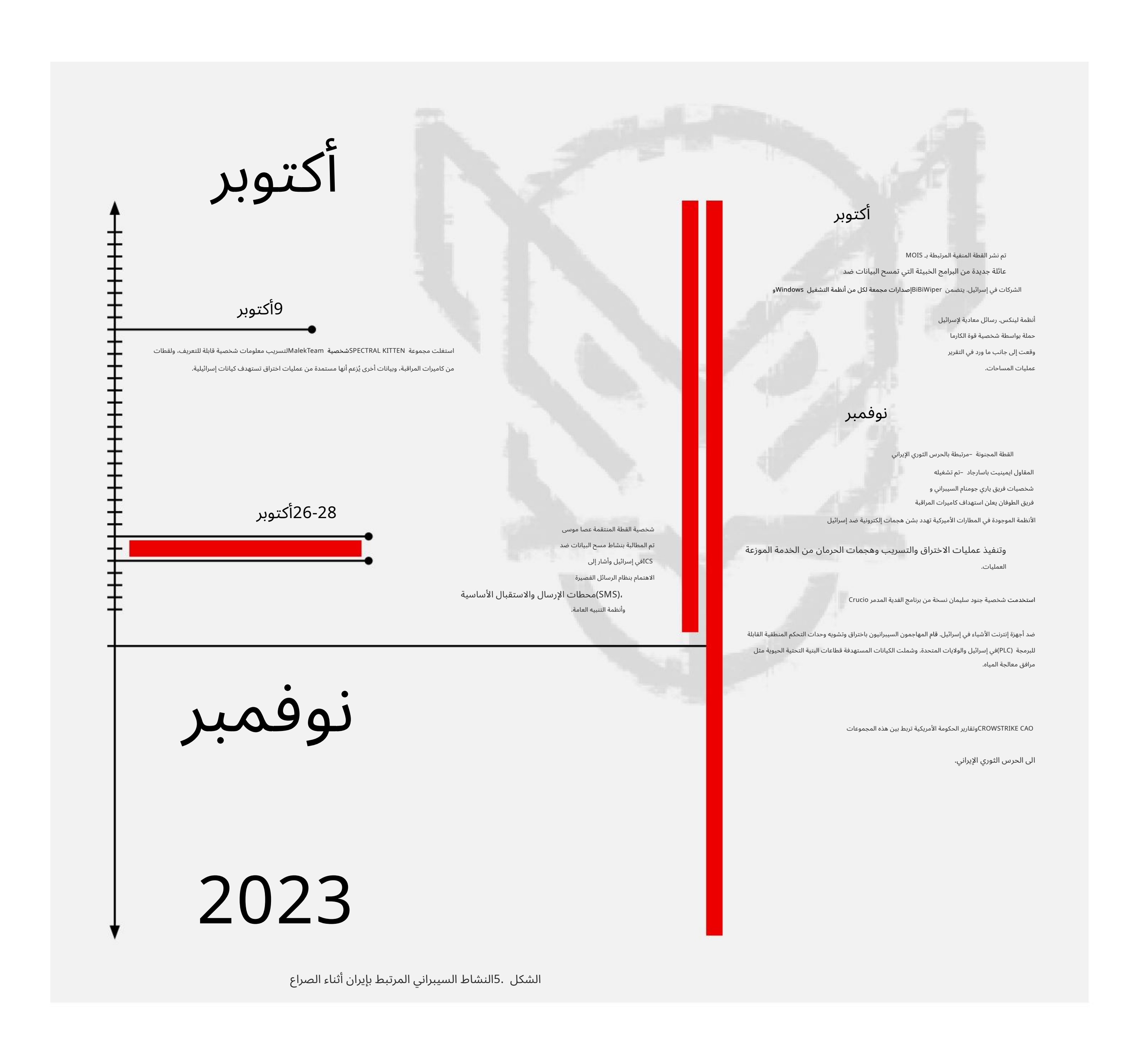
ومن المرجح أن يواصل الهاكرز النشطون استهداف الدول والكيانات خارج منطقة الصراع التي يعتبرونها داعمة لإسرائيل. ويستند هذا التقييم إلى درجة عالية من الثقة استناداً إلى النشاط المستمر الذي لوحظ حتى الآن وفي صراعات مماثلة، مثل الحرب بين روسيا وأوكرانيا، فضلاً عن الاتصالات التي لوحظت داخل قنوات الهاكرز النشطاء.



أعداء إيران يعملون بطريقة غير حقيقية شخصيات للاضطرابات والمعلومات

ولم يلاحظ مركز CrowdStrike CAOأن خصوم إيران المرتبطين بالدولة يقدمون دعمًا تشغيليًا مباشرًا لوحدات حماس الإلكترونية أو العمليات الحركية لكتائب عز الدين القسام. وللخصوم الإيرانيين المرتبطين بوزارة الاستخبارات والأمن في البلاد والحرس الثوري الإسلامي سجل حافل في استخدام الهجمات التخريبية والمدمرة وعمليات الاختراق والتسريب والشخصيات الزائفة ومجموعات القرصنة النشطة لاستهداف الكيانات الإسرائيلية.

ومن المرجح أن يكون هذا النشاط الإلكتروني يهدف إلى التأثير على الجماهير الإسرائيلية خلال الأزمة المستمرة. ورغم أن العمليات الإلكترونية الإيرانية ركزت تاريخيا على إسرائيل، فإن عدد الشخصيات النشطة المزيفة التي يتم استغلالها ضد أهداف إسرائيلية قد زاد منذ اندلاع الصراع بين إسرائيل وحماس. وتركز ادعاءات هذه الشخصيات على تأثير الحملات على التكنولوجيا التشغيلية، ومن المؤكد تقريبا أنها تهدف إلى التأثير على تصور السكان المستهدفين لقدرة الخصوم الإيرانيين على تعطيل الخدمات الحيوية.



الشكل 5.النشاط السيبراني المرتبط بإيران أثناء الصراع

نشاط	التاريخ في عام 2023	الخصم
تسرب المياه من شخصية MALEKTEAM، وكاميرات المراقبة اللقطات والبيانات الأخرى المزعومة مصدرها الاستهداف من خلال الاختراقات الكيانات الإسرائيلية	9 أكتوبر	طيفي هريرة
القطة المجنونة المرتبطة بالحرس الثوري الإيراني المقاول إمينيت باسارجاد، تم تشغيله شخصيات فريق ياري جومنام السيبراني و فريق الطوفان يطالب بنظام كاميرات المراقبة استهداف المطارات الأمريكية، والتهديد بشن هجمات حركية إلكترونية ضد إسرائيل، وتنفيذ عمليات اختراق وتسريب وعمليات DDOS	أكتوبر-نوفمبر	أحمق هريرة
تم نشر القطة المنفية المرتبطة بـ MOIS عائلة البرامج الضارة BIBIWIPER ضد الشركات في إسرائيل؛ قوة الكارما حملة رسائل معادية لإسرائيل حدث ذلك بجانب الماسحة المبلغ عنها العمليات	أكتوبر	منفي هريرة
ادعى موظفو موسى أنهم قاموا بمسح البيانات النشاط ضد أكثر من 20 أنظمة الرقابة الصناعية للشركات (ICS) في إسرائيل والاهتمام الموضح في الرسائل القصيرة ومحطات الإرسال والاستقبال الأساسية أنظمة التنبيه العامة	26-28 أكتوبر	انتقامي هريرة
تم استخدام جنود سليمان المرتبطين بالحرس الثوري الإيراني مجموعة متنوعة من برامج الفدية المدمرة ضد إنترنت الأشياء (IoT) الأجهزة في إسرائيل؛ التابعة للحرس الثوري الإيراني مهاجمو الإنترنت يتعرضون للاختراق والتشويه وحدات التحكم المنطقية القابلة للبرمجة (PLCs) في إسرائيل والولايات المتحدة في وضع حرج كيانات البنية التحتية مثل المياه مرافق العلاج[4]	أكتوبر-نوفمبر	غير منسوب الأشخاص المرتبطون بالحرس الثوري الإيراني
تم نشر جهة فاعلة غير معروفة مرتبطة بإيران مسحات ضد المنظمات الإسرائيلية	19 ديسمبر	مجهول الجهة الفاعلة المرتبطة بإيران
تم إعلان فريق ياري جومنام الإلكتروني المسؤولية عن انقطاع التيار الكهربائي في إسرائيل	25 ديسمبر	قطة مجنونة

4 https://www.cisa.gov/news-events/alerts/2023/12/01/cisa-and-partners-release-joint-advisory-irgc-affiliated-cyber-actors-exploiting-plcs



التوقعات:
العمليات السيبرانية في الصراع

وعلى النقيض من الحرب بين روسيا وأوكرانيا، حيث ساهمت العمليات السيبرانية المعروفة بشكل مباشر في الصراع، فإن أولئك المتورطين في الصراع بين إسرائيل وحماس لم يساهموا بشكل مباشر في العمليات العسكرية لحماس ضد إسرائيل. ومن المؤكد أن النطاق الكامل وتأثيرات النشاط الذي يستهدف إسرائيل، وخاصة من قبل خصوم الدولة الإيرانية والوكلاء المتحالفين معها، غير معروفين بالكامل. ومع ذلك، فإن الحوادث التي تم تحديدها كانت غير متوافقة إلى حد كبير مع المخاوف المبكرة من أن الهجمات السيبرانية الإيرانية قد تتسبب في اضطرابات كبيرة في قطاعات حيوية في إسرائيل وتتوسع في نطاقها إلى الدول الحليفة. وقد يشير هذا الاختلال في التوافق إلى عجز القوات الإيرانية أو افتقارها إلى الاستعداد ورغبتها في تجنب التصعيد غير المقصود الذي قد يجر إيران بشكل أكثر مباشرة إلى الصراع.

يتتبع موقع CrowdStrike CAO مجموعات النشاط Moonshuttle. وSpoiledMocha ويقال إن هذه المجموعات مرتبطة بوكلاء إيران الإقليميين -حركة الحوثيين في اليمن وحزب الله في لبنان على التوالي -على الرغم من أنه لم يتم رصد هذه الكيانات بعد في سياق الصراع بين إسرائيل وحماس.

لقد أظهرت مجموعات القرصنة التابعة للميليشيات الشيعية المؤيدة للعراق تورطًا ثابتًا في استهداف الكيانات الإسرائيلية منذ بداية الصراع. وقد يؤدي التصعيد في الأعمال العدائية الحركية إلى نشاط ذي صلة من جانب هذه المجموعات.

المجموعات.

ومن المؤكد أن نشاط الهاكرز سيستمر بنفس الوتيرة مع التقلبات في التطورات الجيوسياسية ذات الصلة.
تم إجراء هذا التقييم بثقة عالية على أساس أنماط النشاط التي ظهرت حتى الآن وكذلك الأنماط المتسقة التي لوحظت في صراعات مماثلة أخرى.

التهديدات على 2024

مع تخطيط المنظمات للتهديدات المحتملة التي قد تظهر في عام 2024، تبرز في المقدمة عاملان محتملان للاضطراب: الذكاء الاصطناعي التوليدي والانتخابات الحكومية العالمية في عام 2024.

استخدام الذكاء الاصطناعي التوليدي داخل مشهد التهديد

شهدت تكنولوجيا الذكاء الاصطناعي التوليدي المتاحة انتشارًا واسع النطاق في أواخر عام 2022، مما فتح مجالًا جديدًا من الاحتمالات لإنشاء محتوى فعال ولفت انتباه الخصوم الذين يبحثون عن طرق لاستغلال هذه التكنولوجيا الجديدة لأغراضهم الخاصة.

لقد نجح الذكاء الاصطناعي التوليدي في إضفاء الطابع الديمقراطي على الحوسبة بشكل كبير لتحسين عمليات الخصم. كما يمكنه أيضًا أن يخفض حاجز الدخول إلى مشهد التهديد بالنسبة للجهات الفاعلة الأقل تطورًا.

تتضمن منطقتان رئيسيتان لفرص الذكاء الاصطناعي التوليدي ضمن مشهد التهديدات ما يلي:

- تطوير و/أو تنفيذ شبكات كمبيوتر ضارة العمليات (CNO)، بما في ذلك تطوير الأدوات والموارد مثل البرامج النصية أو التعليمات البرمجية التي قد تكون ضارة وظيفيًا إذا تم استخدامها بشكل صحيح
- دعم كفاءة وفعالية الهندسة الاجتماعية وحملات العمليات الإعلامية

»

لقد أصبح الذكاء الاصطناعي التوليدي هائلاً
الحوسبة الديمقراطية
تحسين العمليات المعادية.
يمكن أن يؤدي أيضًا إلى خفض
حاجز الدخول إلى
تهديدات أقل للمناظر الطبيعية
جهات تهديد متطورة.

الذكاء الاصطناعي التوليدي في البرامج الضارة عمليات شبكات الحاسب

من الصعب قياس احتمالية استخدام الخصوم لتقنيات أحدث مثل الذكاء الاصطناعي التوليدي في عملياتهم بثقة، وخاصة فيما يتعلق بكيفية دعم هذه التقنيات للهجمات الخبيثة. ولم تتضمن سوى ملاحظات ملموسة نادرة استخدام الخصوم المحتمل للذكاء الاصطناعي التوليدي خلال بعض المراحل التشغيلية.

من المرجح أن تكون رؤية CrowdStrike لاستخدام مثل هذه الأدوات غير مكتملة.
إما أن يكون هذا نتيجة لملاحظات محدودة، أو حقيقة أن المواد التي تم إنشاؤها بواسطة الذكاء الاصطناعي لم تترك في جوهرها مؤشرات مهمة على طبيعتها الحقيقية، أو أن الخصوم اتخذوا خطوات لتجنب الكشف عن أدلة على استخدام الذكاء الاصطناعي التوليدي.

طوال عام 2023، نادرًا ما تمت ملاحظة الذكاء الاصطناعي التوليدي وهو يدعم تطوير CNO الخبيث و/أو تنفيذه.



إندريك العنكبوت

في فبراير ،2023 استجابت خدمات CrowdStrike لحادث INDRIK SPIDER الذي تضمن RED LockBit أثناء هذا الحادث، استخرج INDRIK SPIDER بيانات اعتماد من مدير بيانات الاعتماد المستند إلى السحابة Azure Key Vault. تُظهر السجلات أن INDRIK SPIDER زار أيضًا ChatGPT أثناء التفاعل مع بوابة Azure.

بالإضافة إلى زيارة ChatGPT أثناء تصفح بوابة Azure — من المفترض لفهم كيفية التنقل في Azure — يشير تحليل نشاط التصفح إلى أن INDRIK SPIDER استخدم محركات البحث مثل Bing وGoogle وقام بالبحث على GitHub أثناء العمليات لفهم كيفية استخراج بيانات اعتماد Azure Key Vault.

يشير استخدام محركات البحث وزيارة ChatGPT إلى أنه على الرغم من أن INDRIK SPIDER ربما يكون جديدًا في السحابة وغير متطور بعد في هذا المجال، إلا أنه يستخدم الذكاء الاصطناعي التوليدي لملء هذه الفجوات المعرفية.



في النصف الثاني من عام ،2023 استخدمت SCATERED SPIDER وحدة Azure AD PowerShell لتنزيل جميع معرفات Entra معرفات المستخدم غير القابلة للتغيير في الخدمات المالية في أمريكا الشمالية الضحية. باستخدام بابها الخلفي ،Entra ID يمكن للمهاجم تسجيل الدخول باسم أي من المستخدمين الذين تم تنزيلهم. يشبه PowerShell المستخدم لتنزيل معرفات المستخدمين غير القابلة للتغيير مخرجات نموذج اللغة الكبير (LLM) مثل تلك الموجودة في ChatGPT.

على وجه الخصوص، نمط التعليق الواحد، والأمر الفعلي ثم سطر جديد لكل أمر

يتوافق مع مخرجات طراز Llama 2 70B.

بناءً على نمط الكود المماثل، SCATERED SPIDER من المرجح أن تعتمد على LLM لإنشاء البرنامج النصي PowerShell في هذا النشاط.



الذكاء الاصطناعي التوليدي في الهندسة الاجتماعية وعمليات المعلومات

في السنوات الأخيرة، تمكنت نماذج لغوية معينة من تأليف قصص خيالية5 وتوليد أعمال فنية رقمية.6 ومنذ منتصف عام 2021 على الأقل، أفادت CrowdStrike بشكل متكرر عن اهتمام بحثي مزعوم بالصور والصوت والفيديو المخادعة للغاية التي تم تصنيعها بواسطة الذكاء الاصطناعي (المعروفة أيضًا باسم "التزييف العميق") من قبل روسيا والصين وإيران. كما تكهن الباحثون والأكاديميون بأن الجهات الفاعلة المهددة ستستخدم بالتأكيد أدوات الذكاء الاصطناعي التوليدية في المعلومات وعمليات التأثير في المستقبل القريب.7

بدأت هذه التكهنات تتحقق في عام 2023: حيث اكتسبت حملة عمليات معلومات صينية، تعتمد على الأرجح على الصور التي ينتجها الذكاء الاصطناعي التوليدي (صور تم إنشاؤها بواسطة نموذج الانتشار على وجه التحديد)، مشاركة حقيقية عبر العديد من منصات التواصل الاجتماعي البارزة طوال شهر سبتمبر. وبخلاف الجهات الفاعلة المرتبطة بالدولة، لاحظت CrowdStrike أيضًا مجموعة من الناشطين الهاكرز تحاول إنشاء أداة للبريد العشوائي باستخدام الذكاء الاصطناعي التوليدي كجزء من جهودها لنشر الرسائل المؤيدة لأذربيجان.

التوقعات

إن الذكاء الاصطناعي التوليدي يتمتع بإمكانات الاستخدام في العديد من المجالات التي من غير المرجح أن يتم تحديدها أو ترويجها في الخطاب العام السائد. ولا شك أن التطوير المستمر للذكاء الاصطناعي من شأنه أن يزيد من قوة إساءة استخدامه المحتملة ــ وخاصة في نطاق عمليات المعلومات وخاصة بالنسبة للجمهور الأقل معرفة بالتقنيات الرقمية. ومن المرجح أن تتكيف الدرجة التي يمكن بها استخدام أدوات الذكاء الاصطناعي التوليدي الشائعة بشكل خبيث مع مرور الوقت مع استجابة الشركات وأصحاب الأدوات والحكومات للتطورات الجديدة وإساءة الاستخدام الملحوظة.

تقدر شركة CrowdStrike CAO أن الذكاء الاصطناعي التوليدي من المرجح أن يُستخدم في الأنشطة السيبرانية في عام 2024 مع استمرار اكتساب التكنولوجيا لشعبية. سيتتبع الفريق بالضبط كيف يستخدم الجهات الفاعلة في مجال التهديد هذه التكنولوجيا، وكيف يختلف هذا الاستخدام عن التطبيقات السائدة. طوال عام 2024. يتضمن هذا النوع من الأبحاث فحص كل من:

- احتمالية استخدام الخصوم لبرامج ماجستير القانون المتاحة للجمهور أو مفتوحة المصدر، وهو ما من المرجح أن يتطلب التنقل المستمر للخصم حول الضمانات ضد النشاط الضار أو غير القانوني (على سبيل المثال، كسر الحماية).

- محاولات الخصوم لتطوير نماذجهم الخاصة أو أدوات الذكاء الاصطناعي التوليدية التي تتطلب هندسة أقل سرعة. والجدير بالذكر أن تكلفة تدريب خبراء الذكاء الاصطناعي يمكن أن تردع بشكل كبير تطويرهم المستقل غير المشروع. وكثيراً ما كانت محاولات الجهات الفاعلة في التهديد لصياغة مثل هذه النماذج واستخدامها في عام 2023 بمثابة عمليات احتيال أدت إلى نتائج ضعيفة نسبياً، وفي كثير من الحالات، سرعان ما أصبحت غير صالحة للاستخدام.

---

5 https://apnews.com/article/7f49bd9aa9d1427d8400e40beb9f5ba4
6 https://apnews.com/article/artificial-intelligence-images-rights-1c6d9e0e260e2d135a3e3bf98d5493df
7 https://cdn.openai.com/papers/forecasting-misuse.pdf

انتخابات 2024

في عام 2024، سيشارك أفراد من 55 دولة يمثلون أكثر من 42% من سكان العالم في الانتخابات الرئاسية والبرلمانية و/أو العامة.

وتشمل هذه الانتخابات سبع دول من بين الدول العشر الأكثر اكتظاظا بالسكان في العالم: الهند والولايات المتحدة وإندونيسيا وباكستان وبنجلاديش وروسيا والمكسيك. كما ستُجرى انتخابات وطنية رفيعة المستوى في دول أو مجموعات متورطة في صراعات جيوسياسية كبرى أو قريبة منها. وتشمل هذه الدول تايوان وأذربيجان والهند وباكستان وإيران وبيلاروسيا وروسيا وفنلندا وليتوانيا والاتحاد الأوروبي.

من المرجح أن تتيح إمكانات عام 2024 لتحويل الجغرافيا السياسية في جميع أنحاء العالم في المستقبل القريب للخصوم فرصًا عديدة، ودفعًا استراتيجيًا كبيرًا، لاستهداف الكيانات المشاركة في العمليات الانتخابية طوال العام المقبل.

استهداف الانتخابات

إن النشاط السيبراني الذي يستهدف الانتخابات قد يتراوح بين المحاولات المباشرة لتعطيل العمليات الانتخابية إلى الجهود غير المباشرة للتأثير على رأي الناخبين نحو النتائج التي يفضلها الخصم.8 إن الاستهداف الأكثر مباشرة، ولكن الأقل تواترا، ينطوي على التطفل على البرامج والأجهزة المستخدمة لتسجيل الأصوات وإحصائها وفرزها ونقلها في أنظمة التصويت. وقد يتراوح هذا الشكل من التدخل في الانتخابات من استخدام هجمات الشبكة الحاسوبية لتعطيل أو إتلاف أو تدمير أنظمة التصويت عمداً إلى استخدام الوصول المتميز أو الثغرات الأمنية لمحاولة تغيير عدد الأصوات دون اكتشافها.

في عام 2024، الأفراد من 55 دولة تمثل أكثر من 42% من سكان العالم سوف يشارك السكان في رئاسي، برلماني و/أو الانتخابات العامة. هذا تتضمن سبعة من العشرة الأكثر الدول الأكثر سكانا في العالم

قد تتضمن الأشكال الأقل مباشرة من الاختراق المستهدف محاولات اختراق أو تعطيل الوصول إلى أو تسريب البيانات من أنظمة الحكومة التي توفر معلومات لوجستية للناخبين أو تخزن بيانات تسجيل الناخبين أو تدعم بطريقة أخرى إجراء انتخابات شفافة وديمقراطية. تشمل جهود الاختراق المستهدفة هذه استخدام هجمات الحرمان من الخدمة الموزعة أو تشويه مواقع الويب ضد أنظمة الحكومة المحلية والبلدية والإقليمية والولائية، وهو تكتيك يفضله تاريخيًا نشطاء القرصنة الذين يسعون إلى تبني وجهات نظرهم خلال اللحظات السياسية المتوترة. الأحزاب الأخرى المشاركة في الانتخابات -

مثل المرشحين السياسيين والأحزاب والجهات المانحة وجماعات المناصرة - يمكن استهدافهم أيضًا بعدة طرق، بما في ذلك عن طريق استخدام عمليات الاختراق والتسريب

في كثير من الأحيان يتم تصميمها لتشويه سمعة الهدف علنًا.

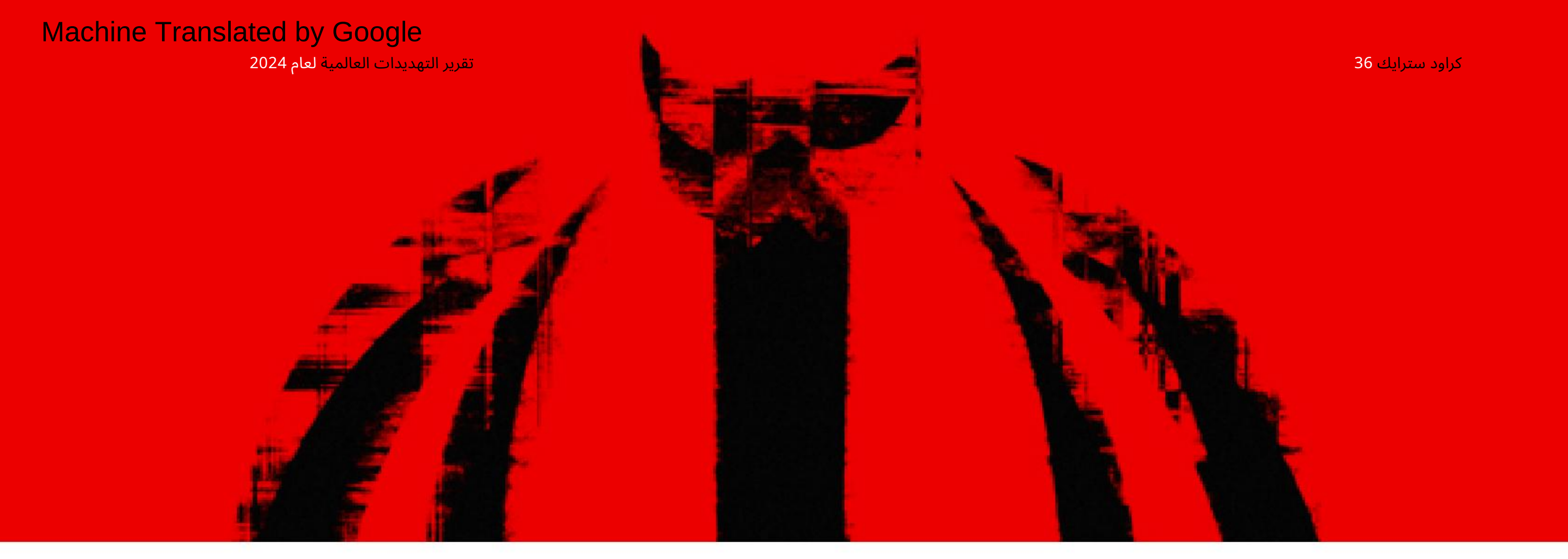
إن النوع الأقل مباشرة من استهداف الانتخابات ـ ولكنه بالتأكيد الأكثر شيوعًا والأصعب منعًا عادةً ـ ينطوي على توزيع معلومات مضللة أو مضللة على الناخبين قبل وأثناء وبعد عمليات التصويت في محاولة لإثارة الشكوك.

للتأثير على الرأي العام.

وقد تتخذ هذه العمليات المعلوماتية أشكالاً عديدة. ومن بين الموضوعات الشائعة محاولات توليد روايات مثيرة للاضطراب ـ على سبيل المثال، قد تعمل هذه العمليات على تقويض ثقة الجمهور في نتائج الانتخابات، وتعزيز تصورات مفادها أن أحزاباً سياسية أو أفراداً بعينهم فاسدون، أو التشكيك في الشخصية الشخصية للمرشحين، أو نشر خطاب اجتماعي تحريضي واستقطابي. وقد تهدف عمليات أخرى إلى تعزيز وجهات النظر التي تصور الجهة المسؤولة عن التهديد في ضوء أكثر إيجابية؛

على سبيل المثال، كمدافع عن مواقف سياسية محددة مفيدة لتلك الكيانات أو ممثل لخطاب التعاون أو التعايش.

8على الرغم من أن هذا القسم يوضح بالتفصيل تصرفات الجهات الفاعلة الخبيثة الخارجية التي تستهدف الانتخابات، إلا أنه من الجدير بالذكر مع ملاحظة أن الحكومات الديمقراطية ظاهريًا تستخدم أحيانًا سلطاتها الأمنية الداخلية أيضًا لتقييد التدفق الحر للمعلومات قانونيًا أثناء دورات الانتخابات (على سبيل المثال، إغلاق الإنترنت والرقابة).



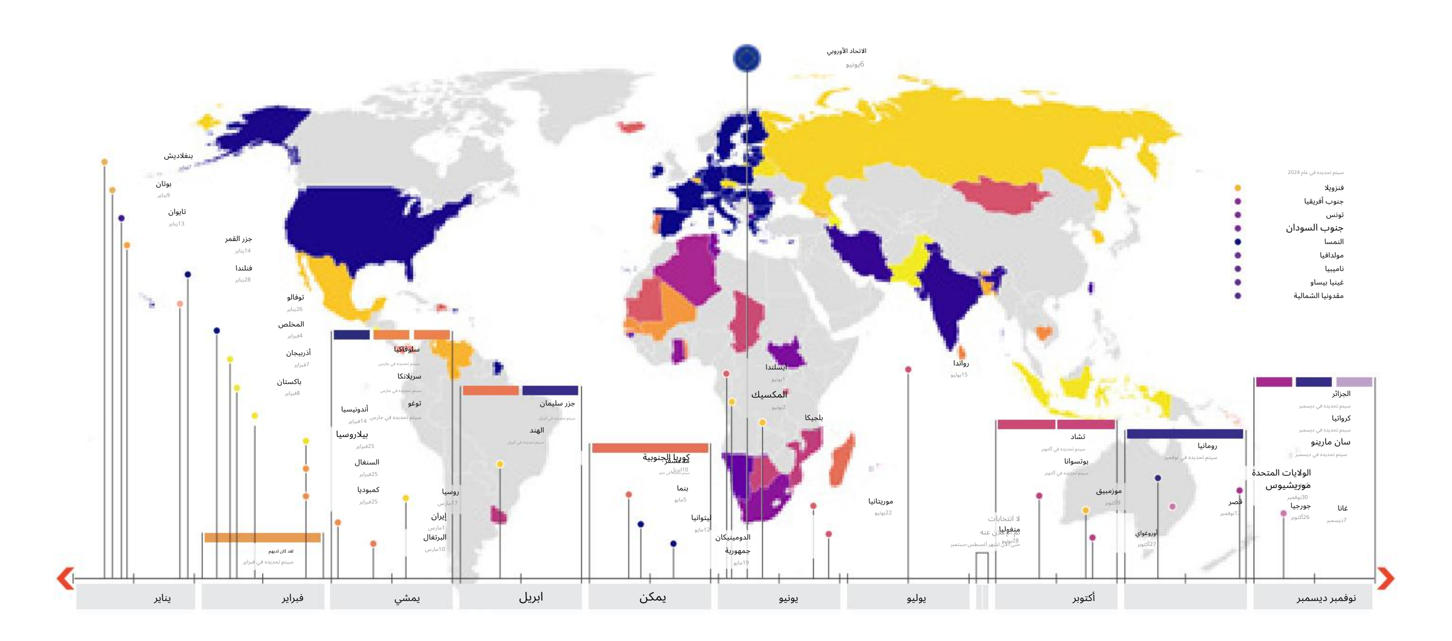
تسليط الضوء على التهديد:

الاستهداف الإيراني للولايات المتحدة الانتخابات في 2020

في أواخر أكتوبر 2020، قبل أسابيع قليلة من دورة الانتخابات الرئاسية الأمريكية الأخيرة، نفذ جهات تهديد إيرانية هجمات إلكترونية مستهدفة متنوعة ضد كيانات أمريكية. أرسلوا رسائل بريد إلكتروني تهديدية إلى الناخبين، زاعمين أنهم يمثلون مجموعة سياسية أمريكية يمينية متطرفة ويوجهون المتلقين للتصويت لمرشح معين. كما نشر جهات تهديد إيرانية مقطع فيديو يزعم زوراً أنه يصور جهات خارجية تقوم بتزوير بطاقات الاقتراع، مما يعني أن حزباً سياسياً معيناً سيسعى إلى استغلال الثغرات الأمنية واختراق أنظمة التصويت.

التوقعات

كانت الأنشطة الخبيثة الأكثر شيوعًا التي تستهدف الانتخابات تاريخيًا
تتضمن عمليات معلوماتية من المحتمل أن تقوم بها كيانات مرتبطة بالدولة ضد مواطني الدول التي تحمل مصلحة جيوسياسية محددة للفاعل المهدِّد
والقرصنة الإلكترونية البسيطة قصيرة الأمد ــ بما في ذلك هجمات الحرمان من الخدمة وتشويه المواقع الإلكترونية ــ ضد كيانات الحكومة المحلية والولائية. ويشهد هذا الاتجاه نمواً سريعاً.
ومن المرجح بشدة أن يستمر ذلك في عام 2024.



الشكل 6. البلدان التي ستجري انتخابات رئاسية أو برلمانية أو عامة في عام 2024

ومن المرجح أن يؤدي الاستقطاب الشامل في الطيف السياسي في العديد من البلدان في ظل استمرار القضايا الاقتصادية والاجتماعية إلى زيادة قابلية مواطني تلك البلدان للتأثر بالإرهاب ــ وخاصة حملات الإرهاب التي تستهدف تعزيز الآراء السلبية لهؤلاء الأفراد تجاه المعارضين السياسيين.

بالإضافة إلى ذلك، فإن التغييرات أو تخفيضات الموظفين التي تؤثر على إمكانية تنفيذ سياسات تعديل المحتوى في شركات وسائل التواصل الاجتماعي الكبرى من المرجح أن توفر فرصًا لاستغلال الخصوم باستخدام هذه المنصات لنشر سرديات الإعلام الخارجي.11

وفي ظل هذه البيئات السياسية القائمة حالياً في أغلب البلدان الكبيرة والمهمة جيوسياسياً، فمن المؤكد تقريباً أن عام 2024 سوف يمثل اختباراً عالمياً صعباً للديمقراطيات.

في عام 2024، من المرجح أن تتعرض البلدان ذات الاهتمام التي تشارك في دورات الانتخابات لخطر حملات إعلامية خارجية كبيرة وطويلة الأمد من قبل القوى العالمية الكبرى. روسيا وإيران

من المرجح أن تستخدم روسيا الحرب ضد الولايات المتحدة والاتحاد الأوروبي، اللذين تعتبرهما من المعارضين الجيوسياسيين الرئيسيين.

ومن المرجح أيضًا أن تشن الصين حملات تحريضية ضد الانتخابات التي تُعقد في نطاق نفوذها الإقليمي المفترض، مثل تلك التي تُعقد في إندونيسيا وكوريا الجنوبية وتايوان. ومن المؤكد تقريبًا أن روسيا ستتصرف على نحو مماثل في الانتخابات التي تُعقد في بيلاروسيا وليتوانيا وفنلندا وجورجيا. ومن المرجح للغاية أن تشن الهند وباكستان حملات تحريضية كبيرة ضد بعضهما البعض خلال الانتخابات التي ستجري في أبريل/نيسان وفبراير/شباط 2024، وخاصة في ظل الاضطرابات السياسية والاستقطاب الحاليين في كلا البلدين.

ونظراً لسهولة استخدام أدوات الذكاء الاصطناعي في توليد روايات خادعة ولكنها مقنعة، فمن المرجح أن يستخدم الخصوم مثل هذه الأدوات لإجراء حملات إعلامية ضد الانتخابات في عام 2024. ومن المرجح أيضاً أن يستخدم الحزبيون النشطون سياسياً داخل البلدان التي تجري فيها الانتخابات الذكاء الاصطناعي التوليدي لإنشاء معلومات مضللة لنشرها داخل بلدانهم.

دوائري الخاصة.

وقد لوحظت هذه المشكلات بالفعل داخل الأسابيع القليلة الأولى من عام 2024، حيث استخدم الممثلون الصينيون المحتوى الذي تم إنشاؤه بواسطة الذكاء الاصطناعي في حملات وسائل التواصل الاجتماعي للتأثير على نشر المحتوى المنتقد للانتخابات الرئاسية في تايوان

مرشحين للانتخابات.

»

من المرجح أن تتعاون روسيا وإيران
استخدام النفوذ ضد الولايات المتحدة
والاتحاد الأوروبي، الذي يعتبرونه
المعارضون الجيوسياسيون الرئيسيون.

9 https://www.eastasiaforum.org/2024/01/06/military-influence-and-policy-peril-in-pakistan/
https://foreignpolicy.com/2024/01/02/india-elections-modi-bjp-congress-nda-lok-sabha-brics/
10 https://www.cambridge.org/core/journals/american-policies-science-review/article/abs/partisan-polarization-is-the-primary-psychological-motivation-3F7D2098CD87AE5501F7AD4A7FA83602/ ما وراء نشر الأخبار الكاذبة سياسيا على تويتر
11 https://www.theguardian.com/media/2023/dec/07/2024-elections-social-media-content-safety-policies-moderation

في شبه جزيرة القرم

منظر جمالي

مؤشر CrowdStrikeللجرائم الإلكترونية® يتتبع (ECX) النشاط -بما في ذلك عدد رسائل البريد الإلكتروني العشوائية التي تم رصدها ومتوسط تكلفة شراء الوصول إلى شبكة الشركة -عبر قطاعات متعددة من نظام eCrimeالبيئي ويحسب العدد الإجمالي لضحايا برامج الفدية التي تم رصدها.

حتى مايو ،2023أظهر مؤشر ECXاتجاهات مماثلة لتلك التي لوحظت في عام 2022.

ومع ذلك، بدءًا من يونيو 2023فصاعدًا، شهد مؤشر ECXنموًا ملحوظًا، مع ارتفاعات كبيرة بين يونيو وأغسطس. وكان من بين المساهمين الأكثر تأثيرًا في هذه الارتفاعات ارتفاع معدل حوادث BGHوزيادة مفاجئة في هجمات DDoSالملحوظة.

سجل مؤشر ECXارتفاعًا جديدًا في نوفمبر ،2023مما يعكس الزيادة في أعداد رسائل البريد الإلكتروني العشوائية وارتفاع متوسط السعر للمحملين والسارقين.

نقاط ضعف جديدة مع
9/10درجة CVSS3
+6%

حوادث BGHالتي تنطوي على
تسريبات البيانات
+76%

متوسط تكلفة المحمل
+169%

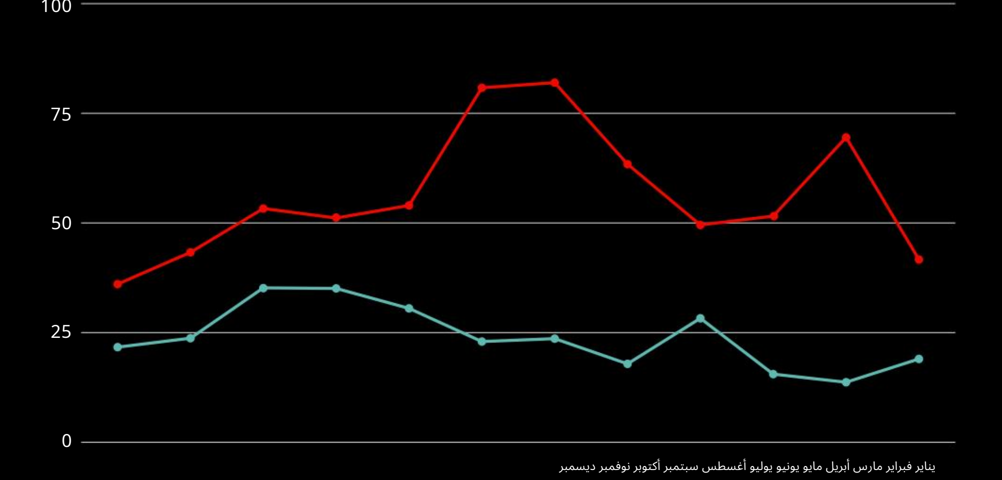
متوسط تكلفة التشفير
+250%

متوسط تكلفة السارق
+286%

متوسط الفدية
يطلب
-27%

تم تحديد البريد العشوائي
رسائل البريد الإلكتروني
-15%

قيمة ECX = +67%



الشكل .7قيمة مؤشر الجرائم الإلكترونية، 2022مقابل ،2023والتغييرات الرئيسية التي يمكن ملاحظتها، 2023

سجل مؤشر ECX لعام 2023 أكبر نشاط سنوي حتى الآن، وهو ما يمثل نمو المؤشر على أساس سنوي. ومن المرجح أن تنخفض رسائل البريد الإلكتروني العشوائية في عام 2023 حيث بحث الخصوم عن وسائل أخرى للوصول الأولي وبعد أن أغلقت عملية متعددة الجنسيات برنامج QakBot التابع لشركة .MALLARD SPIDER

على الرغم من أن متوسط طلب الفدية كان أقل في عام 2023 مقارنة بعام 2022، فمن المرجح أن يمثل هذا قيمة شاذة في مجموعة البيانات وليس رؤية دقيقة لمشهد التهديدات. من المرجح أن تظل طلبات الفدية مرتفعة باستمرار طوال هذه الفترة، لكن القدرة على تتبع هذه القيم أصبحت صعبة بسبب قيام الجهات الفاعلة في مجال التهديد والضحايا بتنفيذ تدابير خصوصية أكثر صرامة فيما يتعلق بمطالبات ومدفوعات أسعار الفدية.

صيد الحيوانات الكبيرة

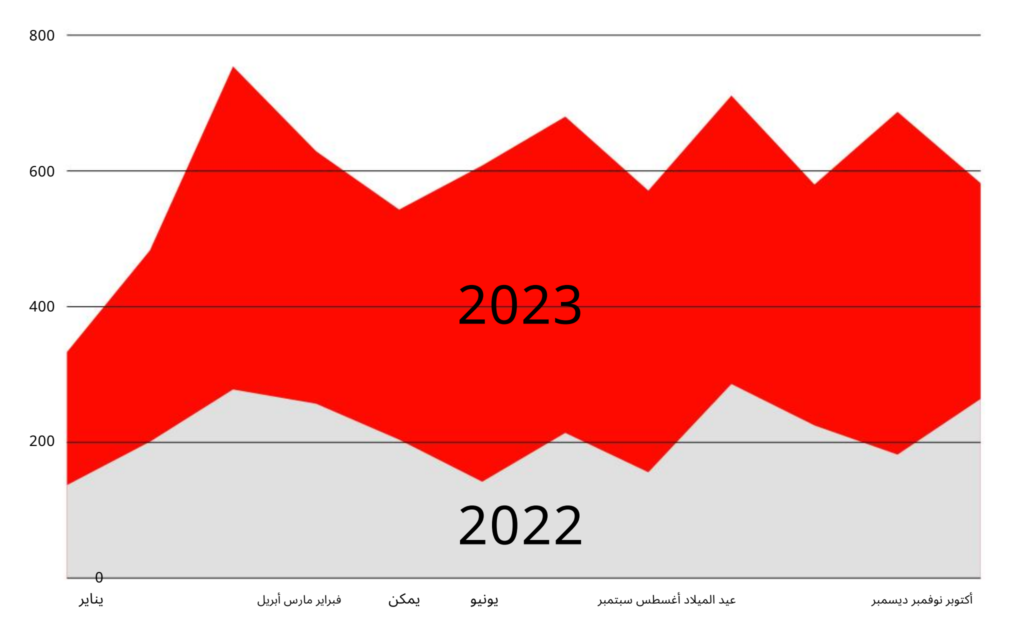
إحصائيات BGH DLS لعام 2023

زاد عدد الضحايا المذكورين على مواقع التسريب المخصصة لـ BGH بشكل كبير في عام 2023، مع نشر 4615 ضحية على - DLSs بزيادة قدرها 76٪ عن عام .2022

وقد ساهم العديد من العوامل في هذا النمو، بما في ذلك خصوم BGH الذين ظهروا حديثًا، ونمو عمليات الخصوم الحالية وحملات مختارة عالية الحجم مثل عمليات استغلال GRACEFUL SPIDER متعددة اليوم.

»

عدد الضحايا الذين تم تسميتهم في مواقع التسرب المخصصة لـ BGH زيادة كبيرة في 2023، مع 4615 مشاركة للضحايا تم تصنيعه خصيصًا لـ — DLSs زيادة بنسبة 76% أكثر من .2022



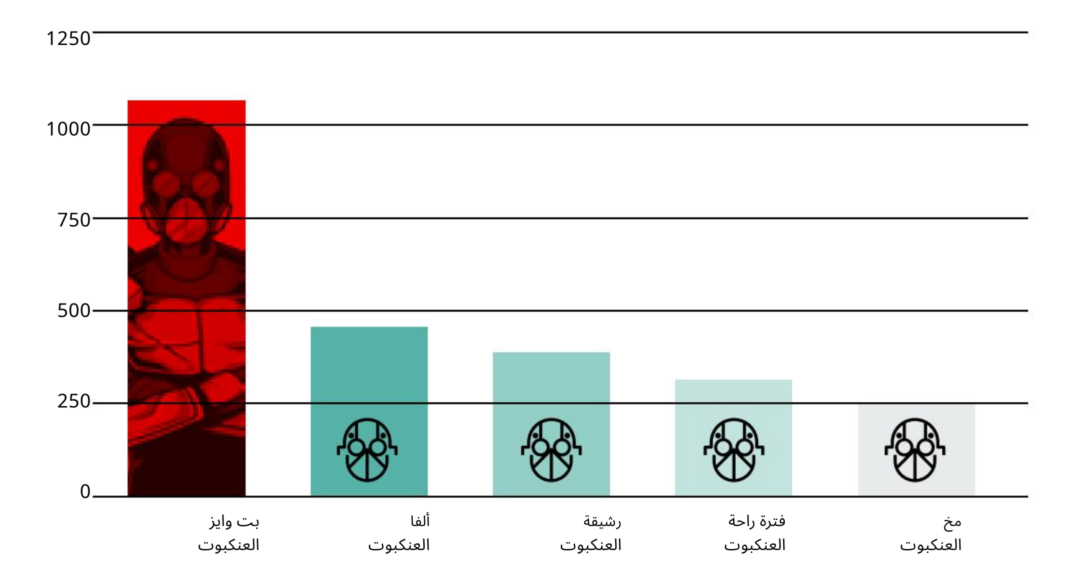
الشكل .8 كمية الوظائف الشاغرة في DLS، 2022 مقابل 2023

بشكل جماعي، شكلت BRAIN SPIDER وRECESS SPIDER وGRACEFUL SPIDER وALPHA SPIDER وBITWISE SPIDER ما يصل إلى 77% من المشاركات عبر جميع أنظمة DLS المعادية التي تم تعقبها.

لقد نشر كل من ALPHA SPIDER وBITWISE SPIDER تاريخيًا العديد من منشورات DLS الجديدة وتم تصنيفهما في المركزين الأول والثاني على التوالي لأعلى عدد من منشورات DLS في عامي 2022 و3202.

بدأت BRAIN SPIDER وRECESS SPIDER عمليات برامج الفدية الخاصة بهما في منتصف عام 2022 ويناير 2023 على التوالي. ومنذ ذلك الحين، اكتسبتا شهرة كبيرة لتحتلا المركز الرابع (RECESS SPIDER) والخامس (BRAIN SPIDER) من حيث عدد المشاركات في DLS في عام 2023.

استغلت — GRACEFUL SPIDER التي تعمل منذ عام 2016 وتدير عادةً حملات ذات حجم منخفض — ثلاث ثغرات أمنية في عام 2023 لاستخراج البيانات من مئات الضحايا في جميع أنحاء العالم. وفي النهاية، نشرت هذه المجموعة ثالث أعلى عدد من منشورات DLS في عام 2023.



الشكل 9. أكبر خمسة خصوم حسب مشاركات DLS، 2023

SCATERED SPIDER يتبنى برامج الفدية كطريقة أساسية لتحقيق الربح

بدأت مجموعة SCATERED SPIDER في استخدام برنامج الفدية Alphv التابع لشركة ALPHA SPIDER في أبريل 2023. كان الخصم قد استغل عمليات الاختراق من قبل عن طريق بيع بيانات الضحايا وتبادل بطاقات SIM بالإضافة إلى سرقة العملات المشفرة. أدى اعتماد برامج الفدية كوسيلة أساسية للابتزاز إلى تغيير نطاق ملف تعريف هدف الخصم: يمكن تصنيف معظم ضحايا SCATTERED SPIDER في عام 2023 إما كأهداف استطلاع أو أهداف تحقيق الدخل. عادةً ما تكون أهداف الاستطلاع مؤسسات تعمل في قطاعات الاستعانة بمصادر خارجية لعمليات الأعمال وإدارة علاقات العملاء وتجربة العملاء والتكنولوجيا والاتصالات. يستخدم SCATTERED SPIDER عمليات الاختراق في شبكات هذه الكيانات لتحديد البيانات التي قد تكون مفيدة في استهداف تحقيق الدخل من جهات خارجية.

إن ملف أهداف تحقيق الدخل لدى الخصم أوسع بكثير. وتشمل الأهداف الأكثر ملاحظة بشكل مباشر الكيانات ذات الإيرادات المرتفعة _ غالبًا من شركات فورتشن _ 500 التي تتخذ من الولايات المتحدة مقرًا لها. وقد حدث ارتفاع ملحوظ في عدد ضحايا الخدمات المالية في أمريكا الشمالية في النصف الثاني من عام 2023.

أهداف أنشطة إنفاذ القانون خصوم BGH

في عام 2023، استهدفت وكالات إنفاذ القانون المختلفة عمليات معادية لـ BGH والحملات الداعمة لها. وتراوحت أفعالها من اعتقال أفراد معاديين مشتبه بهم إلى تعطيل البنية التحتية المعادية تقنيًا.



















الشكل 10. نشاط إنفاذ القانون ضد BGH والعمليات الداعمة، 2023

في يناير 2023، أسفرت عملية إنفاذ القانون الدولية المنسقة عن الاستيلاء على البنية التحتية لـ HIVE SPIDER والاستحواذ على **مفتاح فك تشفير** Hive ransomware. وبحسب ما ورد، حافظت وزارة العدل الأمريكية على الوصول إلى البنية التحتية الداخلية لـ HIVE SPIDER منذ يوليو 2022 وقدمت منذ ذلك الحين مفاتيح فك التشفير لأكثر من 300 ضحية في جميع أنحاء العالم، مما منع دفع فدية بلغ مجموعها 130 مليون دولار أمريكي. لم يتم ملاحظة أي نشاط لـ HIVE SPIDER منذ يناير 2023؛ ومع ذلك، **انتقلت الشركات التابعة** لـ Hive منذ ذلك الحين إلى عمليات أخرى لبرامج الفدية كخدمة (RaaS).

في فبراير وسبتمبر 2023، أصدرت جهات إنفاذ القانون عقوبات ضد أعضاء WIZARD SPIDER بهدف تقييد أموال الأفراد المذكورين وسفرهم وأصولهم وتعطيل عمليات الخصم أثناء عمله للتحايل على القيود.

في مارس 2023، أعلنت يوروبول عن اعتقال اثنين من المشتبه بهم في عضوية DOPPEL SPIDER الأساسية. وفي يونيو 2023، أعلنت وزارة العدل عن اعتقال شخص يشتبه في أنه تابع لـ BITWISE SPIDER. في أغسطس 2023، أعلن مكتب التحقيقات الفيدرالي عن عملية متعددة الجنسيات - باستخدام حمولة مخصصة لإرسال أمر إيقاف التشغيل - والتي أزالت برنامج QakBot الخبيث التابع لـ MALLARD SPIDER من أكثر من 700000 مضيف واستولت على كمية كبيرة من العملات المشفرة. كما استخدمت WANDERING SPIDER برنامج QakBot التابع لـ MALLARD SPIDER.

في أكتوبر 2023، أعلنت وكالات إنفاذ القانون أنها أسقطت لعبة Ragnar Locker DLS التابعة لـ VIKING SPIDER وألقت القبض على مشتبه به في لعبة Ragnar Locker
في نوفمبر 2023، أعلنت يوروبول أيضًا أنها ألقت القبض على أفراد مرتبطين بممثل برامج الفدية غير المسمى. أخيرًا، في ديسمبر 2023، استولى مكتب التحقيقات الفيدرالي على البنية التحتية لـ ALPHA SPIDER، بما في ذلك Alphv DLS - برنامج الفدية SCATTERED SPIDER المستخدم طوال معظم عام 2023.

عرض مكتب التحقيقات الفيدرالي **أداة فك تشفير** Alphv على أكثر من 500 ضحية لـ ALPHA SPIDER، مما دفع ALPHA SPIDER إلى نقل DLS ولوحة التحكم التابعة لها إلى مواقع Tor جديدة أثناء محاولتها استعادة السيطرة على البنية التحتية المخترقة. ثم قامت ALPHA SPIDER بإزالة قيود الاستهداف من الشركات التابعة، باستثناء الحظر المفروض على استهداف الكيانات داخل رابطة الدول المستقلة.

تحسين سرقة البيانات والابتزاز

منذ عام 2019، هدد خصوم BGH بنشر البيانات المسروقة على DLSs كوسيلة ابتزاز ثانوية بالتنسيق مع نشر برامج الفدية.[21] في عام 2023، واصل الخصوم ابتكار أساليب استغلال لسرقة بيانات الضحايا وزيادة الضغط على الضحايا، مع تبني العديد منهم - بما في ذلك SPIDER - MASKED وGRACEFUL SPIDER سرقة البيانات كوسيلة وحيدة للابتزاز.

كان GRACEFUL SPIDER هو أكثر الجهات المسؤولة عن سرقة البيانات والابتزاز في عام 2023. استغل الخصم ثغرات اليوم صفر في تطبيقات نقل الملفات MOVEit Transfer وGoAnywhere Managed File Transfer بالإضافة إلى برنامج إدارة تكنولوجيا المعلومات SysAid On-Premise. لم يتم ملاحظة نشر برنامج الفدية Clop من GRACEFUL SPIDER في نطاق هذه الحملات، على الرغم من أن الخصم قام باستخراج ونشر البيانات إلى DLS الخاص به والتي تنتمي إلى أكثر من 380 منظمة ضحية. للسماح لجمهور أوسع بالوصول إلى التسريبات، نشر GRACEFUL SPIDER أيضًا بيانات الضحايا على نطاقات الويب الواضحة، وهي تقنية استخدمت لأول مرة بواسطة

أحد الشركات التابعة لـ ALPHA SPIDER في عام 2022.

لقد قام خصوم BGH تاريخيًا وبشكل عشوائي باستخراج ونشر بيانات الضحايا المسروقة. في عام 2023، أظهر هؤلاء الفاعلون في مجال التهديد تركيزًا أكبر على البيانات المسروقة في محاولة لتعظيم الضغط على الضحايا، كما هو موضح في ما يلي:

- نشر بيانات اعتماد مسؤول المجال للضحية وعناوين IP للنظام على Black Basta RaaS DLS. يمكن أن يستغل جهات تهديد مختلفة هذه البيانات لاستهداف المنظمات الضحية.

- إنشاء منشورات منفصلة للضحايا للمؤسسات الخارجية التي تم تحديد بياناتها في شبكة الضحايا ولكن لم تخضع للاختراق.

- قامت العديد من الشركات التابعة لـ RaaS باختراق كيانات الرعاية الصحية العقلية والجسدية وسلطت الضوء على وصولها إلى البيانات والسجلات الحساسة - وقدمت معاينات لها - في منشورات DLS.

- استمر VICE SPIDER في استخدام برنامج نصي PS لأتمتة استخراج البيانات ولكن تم تخصيص البرنامج النصي للبحث عن أسماء الدليل والملفات التي تحتوي على سلاسل مثل *العنف* و*الإساءة* و*السرقة* و*السطو* و*الإذلال* و*التحرش* و*الموت*، ومن المرجح أن يتم التعرف على البيانات التي تشكل إمكانية عالية لإحراج منظمات الضحايا.

لقد عانى العديد من الخصوم، بما في ذلك MASKED SPIDER، وGRACEFUL SPIDER من عيوب تشفيرية في برامج الفدية التي تمكنهم من فك التشفير بسهولة في ظل ظروف معينة. وعلى النقيض من ذلك، توفر سرقة البيانات والابتزاز لجهات BGH طريقًا أسهل لتحقيق الربح. ويسرق العديد منهم ببساطة البيانات من مضيف واحد أو تطبيق يواجه الجمهور. يقدر CrowdStrike CAO أن خصوم BGH من المرجح أن يستمروا في أن يصبحوا أكثر استهدافًا في سعيهم للحصول على البيانات مع إمكانية عالية لإحراج الضحايا.

---

12 https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

التوقعات

يوضح العدد القياسي للضحايا الذين تم ذكر أسمائهم على DLSs طوال عام 2023 مكانة BGH باعتبارها التهديد الإلكتروني الأكثر أهمية حاليًا للمؤسسات في جميع المناطق الجغرافية والصناعات. ويرجع هذا الارتفاع إلى عوامل مختلفة، بما في ذلك حملات استغلال اليوم صفر من GRACEFUL SPIDER، واستمرار خصوم BGH في استهداف الأجهزة غير المدارة -مثل أجهزة البوابة الطرفية للوصول الأولي واستهداف VMware ESXi للتشفير- والعدد المتزايد من الخصوم الذين يطلقون أسماء الضحايا بعد حوادث سرقة البيانات التي لم تشمل نشر برامج الفدية.



رقم قياسي في عدد الضحايا

تم تسميتها على DLSs طوال عام 2023

يوضح وضع BGH كـ

الأكثر أهمية في الوقت الحالي

الجرائم الإلكترونية تشكل تهديدًا للمنظمات

في جميع المناطق الجغرافية

والصناعات.

على الرغم من أن CrowdStrike CAO تقدر أن برامج الفدية ستظل على الأرجح الطريقة الأساسية للابتزاز حتى عام 2024، فإن خصوم BGH سيؤكدون بشكل متزايد على استغلال البيانات المسروقة كوسيلة للضغط على الضحايا لإجبارهم على الدفع.

وهذا صحيح بشكل خاص لأن قواعد لجنة الأوراق المالية والبورصة الأمريكية (SEC) تؤثر على الكشف عن حوادث الأمن السيبراني الكبرى.31

لقد أكد برنامج الفدية Alphv الذي أطلقته SCATTERED SPIDER على فعالية الابتزاز كتكتيك طوال عام 2023. وعلى الرغم من أن SCATTERED SPIDER كانت تجني الأموال من الحملات من خلال سرقة العملات المشفرة ومبادلة بطاقات SIM، فإن برامج الفدية هي تكتيك أكثر انتهازية، مما يسمح للعدو بتوسيع نطاق هدفه. وباستثناء أي نشاط ناجح لإنفاذ القانون يستهدف العدو، فمن المرجح أن يظل SCATTERED SPIDER يشكل تهديدًا خطيرًا للكيانات ذات الإيرادات المرتفعة في القطاع الخاص في عام 2024، وخاصة تلك الموجودة في أوروبا وشمال إفريقيا.

أمريكا.

استهدفت عمليات إنفاذ القانون الدولية المنسقة الجهات الفاعلة في BGH في عام 2023. وشملت هذه اعتقالات للأفراد المعارضين، واتخاذ إجراءات فنية ضد قدرات مختلفة، ومصادرة العملات المشفرة ومعاقبة أفراد محددين.

تعطيل خدمة Hive RaaS من HIVE SPIDER وخدمة QakBot التمكينية من MALLARD SPIDER
لقد تركت البرمجيات الخبيثة فجوات تم ملؤها بسرعة من قبل الجهات المتنافسة في مجال RaaS والبرمجيات الخبيثة كخدمة (MaaS)، مما يدل على قدرة نظام eCrime على الصمود ضد عمليات الإزالة التي لا تؤدي إلى اعتقال الأفراد الذين يقفون وراء العمليات.

13 https://www.sec.gov/news/press-release/2023-139

تمكين الجرائم الإلكترونية

اتجاهات توصيل البرامج الضارة التالية تصحيح Mark-of-the-Web على ملفات ISO

قام الخصوم في عام 2023 بتجربة طرق توصيل البرامج الضارة التي لا تعتمد على وحدات الماكرو أو ملفات ISO، وذلك بعد الزيادة الحادة في استخدام ملفات ISO لتوصيل البرامج الضارة والتصحيح اللاحق الذي قامت به Microsoft لثغرة تجاوز Mark-of-the-Web في ملفات الحاويات في عام 2022.

ارتفع عدد حملات البرامج الضارة التي تستخدم ملفات OneNote الضارة للوصول الأولي بشكل كبير 41 بين أواخر ديسمبر 2022 ومارس 2023، حيث كان من أوائل المتبنين لهذه التقنية المجرمين الذين يوزعون سارقي المعلومات والبرامج الضارة السلعية. وبحلول منتصف يناير 2023، بدأ موزعو البرامج الضارة على نطاق واسع مثل LUNAR SPIDER وHONEY SPIDER وMALLARD SPIDER في استخدام ملفات OneNote كطريقة أساسية لتوزيع البرامج الضارة. في مارس 2023، أعلنت Microsoft عن تغيير من شأنه منع تضمين أنواع الملفات التي يسيء الخصوم استخدامها بشكل شائع في ملفات OneNote.15 بعد الإعلان، انخفضت شعبية ملفات OneNote داخل حملات الخصوم بسرعة.

على الرغم من عدم ظهور تقنية واحدة كمرشحة رائدة لاستبدال ملفات OneNote، إلا أن الخصوم يواصلون تجربة أساليب توصيل البرامج الضارة. وقد استخدم الخصوم مثل HERMIT SPIDER وAPOTHECARY SPIDER وLUNAR SPIDER باستمرار الإعلانات الضارة وتسميم تحسين محرك البحث (SEO).

يستخدم الخصوم الذين يعتمدون على حملات البريد العشوائي تقنيات وأنواع ملفات متعددة لتوصيل البرامج الضارة. استخدم العديد من الخصوم ملفات PDF تحتوي على روابط لملفات مستضافة على عناوين URL خارجية بالإضافة إلى تهريب HTML. تضمنت التقنيات الأكثر حداثة استخدام ملفات WebDAV لتوزيع الحمولات. بحلول نهاية عام 2023، تم توزيع العديد من عائلات البرامج الضارة في طعوم جديدة تحتوي على تحديثات متصفح مزيفة.

الإعلانات الخبيثة وتسميم محركات البحث

إن الإعلانات الخبيثة هي تقنية يستخدمها الجهات الفاعلة في التهديد لإنشاء إعلانات ضارة لتسهيل النشاط الإجرامي. يستخدم الخصوم التسميم المحسن لمحركات البحث للترويج بشكل زائف لمواقع الويب الضارة في مراتب أعلى في نتائج محرك البحث. وعلى غرار الإعلانات الخبيثة، يعتمد التسميم المحسن لمحركات البحث على اعتقاد المستخدمين بأن النتائج الأقرب إلى أعلى نتيجة بحث هي الأكثر مصداقية.

طوال عام 2023، أساءت جهات معادية مثل LUNAR SPIDER استخدام إعلانات Google بانتظام لضمان ظهور إعلاناتها الضارة في أعلى صفحات نتائج البحث. كما استخدمت جهات تهديد مثل مشغلي SolarMarker بانتظام عمليات تسميم محركات البحث طوال عام 2023.

---

14 https://www.crowdstrike.com/blog/qakbot-ecrime-campaign-leverages-microsoft-onenote-for-distribution/
15 https://learn.microsoft.com/en-us/deployoffice/security/onenote-extension-block

زيادة استخدام البرامج الضارة لنظام التشغيل macOS

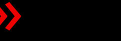
طوال عام 2023، ظهرت العديد من متغيرات البرامج الضارة لنظام التشغيل macOS — بما في ذلك macOS Stealer (AMOS) — COOKIE SPIDER's Atomic وShadowVault وPrivate MacOS Stealer وMacOS Stealer في الأسواق السوداء. جميع عائلات البرامج الضارة لنظام التشغيل macOS التي تم رصدها هي سارقو معلومات قادرين على حصاد كلمات المرور المخزنة وملفات تعريف الارتباط ومحافظ العملات المشفرة.

قام عملاء AMOS بتوزيع هذه الأدوات عبر تسميم محركات البحث بالإضافة إلى الألعاب المزيفة التي يتم لعبها لكسب المال وإعلانات الوظائف غير المشروعة. MacOS Stealer
أشاد العملاء، بما في ذلك الشركات التابعة لبرامج الفدية ALPHA SPIDER، وROYAL SPIDER وBITWISE SPIDER بالسارق. وعلى الرغم من أن COOKIE SPIDER صرحت بأن جزءًا من عملائها الحاليين الذين يتراوح عددهم بين 50 إلى 100 يشمل الشركات التابعة لبرامج الفدية ALPHA SPIDER، وBITWISE SPIDER فإن CrowdStrike CAO لا يمكنها حاليًا التحقق من هذا الادعاء.

اكتسب سارقو نظام التشغيل macOS زخمًا في منظومة eCrime طوال عام 2023 نظرًا لقدرتهم على تمكين الجهات الفاعلة الانتهازية والشركات التابعة لبرامج الفدية أثناء العمليات الإجرامية. ونظرًا لأن غالبية سارقي المعلومات يستهدفون عادةً أنظمة التشغيل المستندة إلى Windows، فقد أدى العدد المتزايد من سارقي نظام التشغيل macOS في منظومة eCrime إلى توسيع فرص الربح في eCrime.

تستمر شركة Access Brokers في تقديم الخدمات باستمرار فرص الوصول

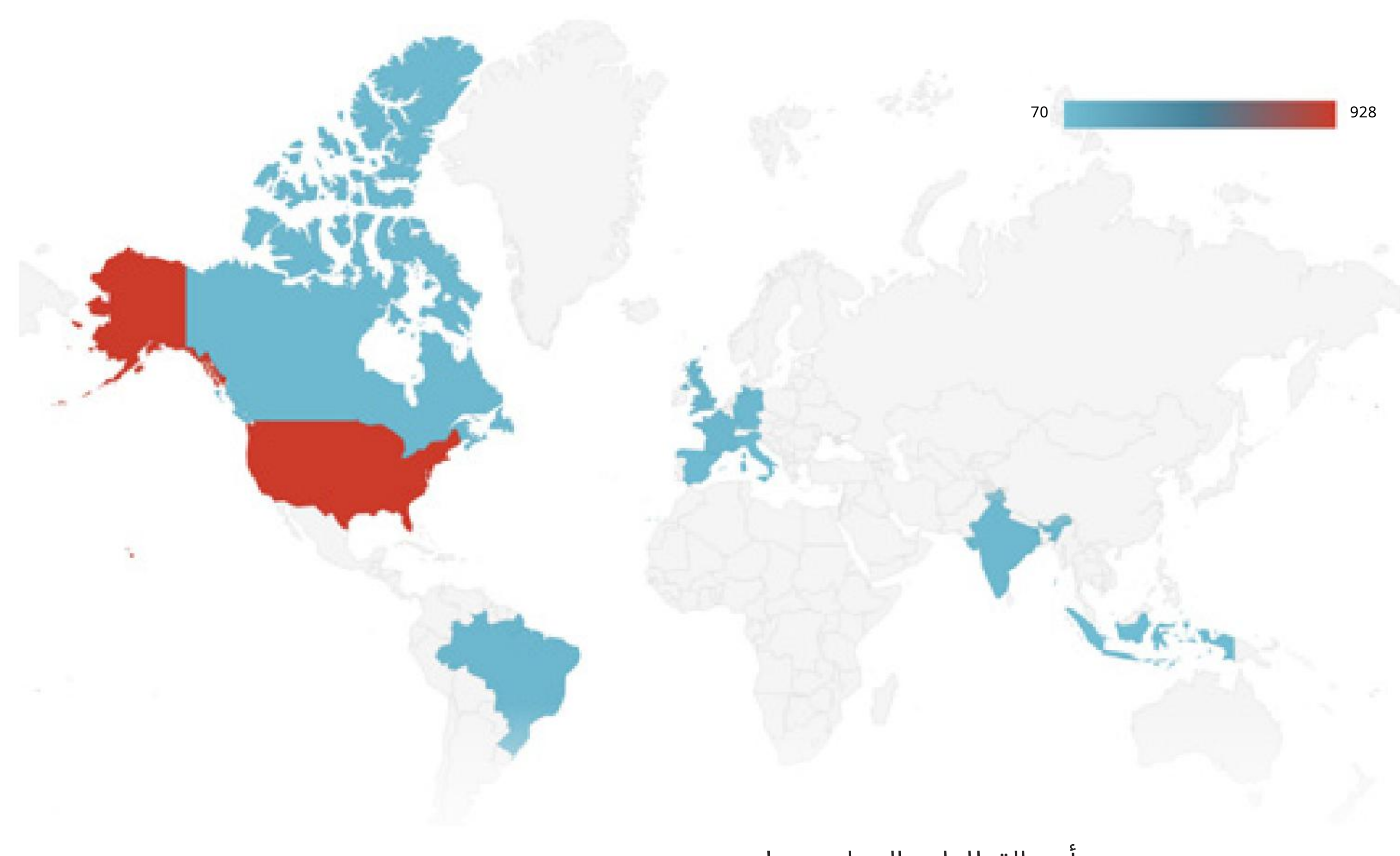
استمر وسطاء الوصول في الاستفادة من توفير الوصول الأولي إلى مجموعة متنوعة من الجهات الفاعلة في مجال الجرائم الإلكترونية في عام 2023، مع زيادة عدد عمليات الوصول المعلن عنها بنسبة 20% مقارنة بعام 2022. وكان القطاع الأكاديمي هو الأكثر إعلانًا، وتجاوزت الإعلانات الخاصة بالكيانات التي تتخذ من الولايات المتحدة مقراً لها جميع المناطق الأخرى. كانت إجراءات الوصول الأولية التي لوحظت في عام 2023 متسقة نسبيًا مع تلك المستخدمة في عام 2022 واستهدفت بانتظام بيانات الاعتماد المخترقة وأساءت استخدامها.



استمرت شركة ACCESS BROKERS في الربح من تقديم المبدئي الوصول إلى مجموعة متنوعة من الجرائم الإلكترونية الجهات الفاعلة المهددة في عام 2023، مع عدد مرات الوصول المعلن عنها زيادة بنسبة 20% مقارنة إلى 2022.

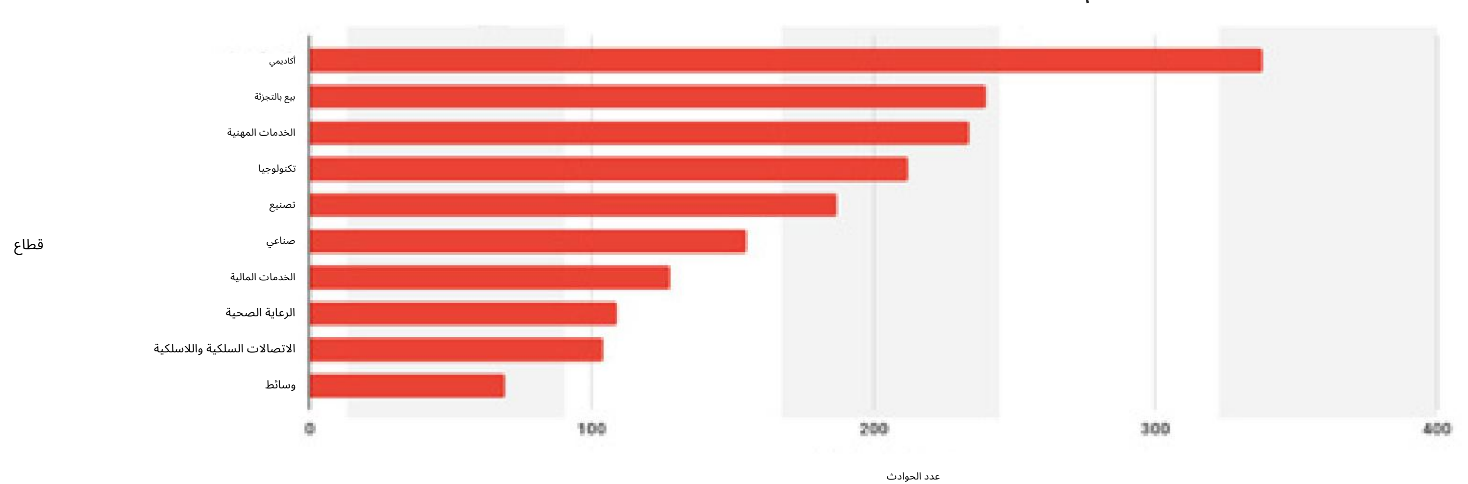
أفضل وسيط للوصول

الإعلانات حسب البلد 2023



أهم القطاعات المعلن عنها

بقلم أكسس بروكرز 2023 |



الشكل .11أفضل 10دول وقطاعات يتم الإعلان عنها من قبل وسطاء الوصول، 2023

التوقعات

إن ظهور البرامج الضارة على نظام التشغيل macOS وتطور تقنيات توصيل البرامج الضارة يوضحان الطبيعة المبتكرة لنظام الجرائم الإلكترونية. وعلاوة على ذلك، يقوم مرتكبو الجرائم الإلكترونية بانتظام بنسخ التكتيكات الناجحة التي يستخدمها المجرمون الآخرون، كما يتضح من زيادة ملفات OneNote لتوصيل البرامج الضارة.

من المرجح أن يستمر ممكّنو الجرائم الإلكترونية في الابتكار وتقديم منتجات جديدة في الأسواق الإجرامية في عام 2024. تم إجراء هذا التقييم بثقة عالية بناءً على الاتجاهات التاريخية في نظام الجرائم الإلكترونية. من المرجح أن تستمر اتجاهات توصيل البرامج الضارة في التقلب، مع استمرار تسميم محركات البحث والإعلانات الضارة في الانتشار، ومواصلة الخصوم المعتمدين على البريد العشوائي تجربة طرق مختلفة بانتظام. تم إجراء هذا التقييم بثقة عالية بناءً على اتجاهات توصيل البرامج الضارة التي لوحظت منذ نهاية عام 2022.

لا تظهر أي علامة فورية على تراجع تهديد سماسرة الوصول. ومن المؤكد أن هؤلاء الجهات الفاعلة في مجال التهديد سوف تسهل عمليات الاختراق لمختلف المنظمات في جميع أنحاء العالم طوال عام 2024 باستخدام مزيج من الأساليب والتقنيات والتكتيكات الراسخة إلى جانب الأدوات الأساسية والأدوات المخصصة.

الجرائم الإلكترونية المستهدفة

الخصوم يواصلون المشروعية استخدام أداة RMM

على مدار عام 2023، استخدم العديد من مرتكبي الجرائم الإلكترونية المستهدفة - وخاصة SOLAR SPIDER وDISTANT SPIDER وCHEF SPIDER - أدوات المراقبة والإدارة عن بعد (RMM) المشروعة على نطاق واسع.

بدءًا من مارس 2023، تبنت CHEF SPIDER تكتيكات هندسية اجتماعية متطورة لتوجيه الضحايا إلى تنزيل برامج التثبيت ClickOnce وInno Setup لأداة RMM ConnectWise ScreenConnect. وعلى الرغم من أن CHEF SPIDER استهدفت تاريخيًا أنظمة نقاط البيع في قطاع الضيافة من خلال اختراق الخوادم المتصلة بالإنترنت، فقد تحول الخصم تدريجيًا إلى استهداف مقدمي خدمات قطاع الضيافة ومقدمي الخدمات المالية وشركات التسويق الرقمي في الولايات المتحدة طوال عام 2023.

في عام 2023، استمرت — DISTANT SPIDER التي تعتمد بشكل كبير على ConnectWise ScreenConnect — في نشر مثبتات MSI (المعروفة أيضًا باسم مثبتات Windows) لأداة RMM المشروعة هذه بعد استغلال خوادم الإنترنت الضعيفة داخل بيئات الضحايا. في سبتمبر 2023، من المحتمل أن يكون اختراق سابق لـ DISTANT SPIDER ConnectWise ScreenConnect قد مكّن أحد الشركات التابعة لـ ALPHA SPIDER من استخراج البيانات والمطالبة بفدية من الضحية.

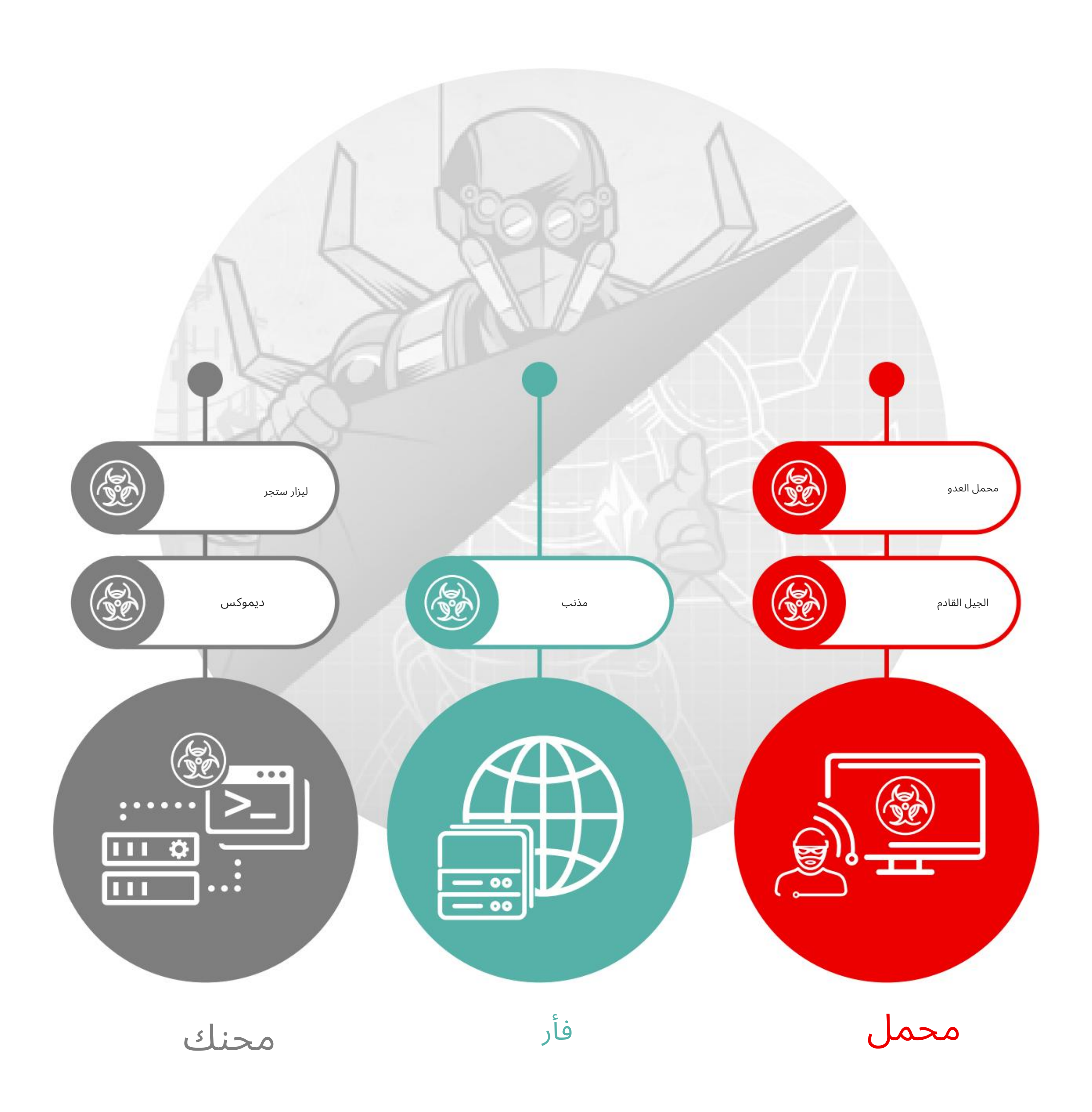
في يونيو 2023، من المرجح أن يكون SOLAR SPIDER قد استخدم رسائل البريد الإلكتروني الاحتيالية لتوجيه الضحايا لتنزيل أرشيف ZIP المستضاف على GitHub. يحتوي هذا الأرشيف على أداة تحميل تستغل اختطاف ترتيب البحث في DLL لتشغيل أداة RMM Remote Management System المشروعة. وقد استخدمت SOLAR SPIDER أداة RMM المشروعة NetSupport Manager منذ أكتوبر 2022 على الأقل.

البرامج الخبيثة التاريخية CARBON SPIDER

موزعة في حملات ذات حجم منخفض

طوال عام 2023، استخدم مرتكبو الجرائم الإلكترونية العديد من عائلات البرامج الضارة التي كانت حصرية في السابق لـ CARBON SPIDER (الشكل 12). ومنذ أن استخدم بائعو MaaS غير النشط هذه العائلات في عامي 2022 و3202، لا يمكن نسب أي من هذه الحملات إلى CARBON SPIDER غير النشط الآن؛ ومع ذلك، توضح الحملات الشعبية المستمرة للأدوات. وعلى النقيض من مشغلي MaaS النموذجيين، يشير الحجم المنخفض للحملات التي تستخدم الأدوات على الأرجح إلى منح عدد قليل فقط من العملاء إمكانية الوصول.

جودسوفت



الشكل 12. أدوات CARBON SPIDER القديمة المستخدمة في عام 2023

التركيز الإضافي على أمريكا اللاتينية

تم تحديد الخصوم

في عام 2023،أطلقت شركة CrowdStrike CAO اسمًا على ثلاثة أعداء جدد لبرنامج SPIDER يركزون بشكل أساسي -ولكن ليس حصريًا - على أمريكا اللاتينية SQUAB SPIDER وROBOT SPIDER وODYSSEY SPIDER :(LATAM)(الشكل 13).بما في ذلك BLIND SPIDER الذي تم تحديده سابقًا، يركز أربعة أعداء لبرنامج ISPIDER الآن على استهداف أمريكا اللاتينية.



الشكل 13.خصوم SPIDER الذين يركزون على أمريكا اللاتينية

استخدمت كل من ODYSSEY SPIDER وBLIND SPIDER وAVIATOR SPIDER خدمة التشفير Fsociety من ROBOT SPIDER خلال عام 2023. تتكون أدوات Fsociety عادةً من مجموعة من البرامج النصية التي تقوم بتنزيل وتنفيذ حمولة TEN. وسيطة والتي تقوم بعد ذلك بتحميل حمولة RAT نهائية في الذاكرة. طوال عام 2023، استمرت ROBOT SPIDER في تحديث تشفير Fsociety لتحسين التعتيم وإضافة القدرات. بشكل عام، بلغت سلاسل العدوى التي تستفيد من Fsociety ذروتها في أدوات RAT مثل njRAT Lime.

يستخدم ODYSSEY SPIDER، الذي من المرجح أن يكون مقره في البرازيل، نظام Fsociety الخاص بـ ROBOT SPIDER تركز ODYSSEY SPIDER بشكل أساسي على قطاعي السفر والضيافة في أمريكا اللاتينية وجنوب شرق أوروبا، وتهدف بشكل خاص إلى تحقيق الدخل من تفاصيل بطاقات الدفع المدخلة أثناء عمليات الحجز المتعلقة بالسفر. ومع ذلك، في الربع الثالث من عام 2023، بدأ الخصم في استهداف العديد من القطاعات والمناطق الأخرى، على الأرجح مع الاستفادة من فترات الإقرار الضريبي المحلية.

يستهدف SQUAB SPIDER في المقام الأول المؤسسات المالية، وخاصة تلك التي تتخذ من المكسيك مقراً لها، ولكن ليس حصرياً. ويحقق الخصم الوصول الأولي من خلال استغلال خوادم الويب لنشر مجموعة واسعة من قذائف الويب. ومن هناك، يعتمد الجهات الفاعلة المهددة على قذائف ربط BLUEAGAVE السلبية أو المستمعين البسطاء لتمكين الحركة الجانبية عبر الشبكة وتجنب حركة C2 التقليدية بشكل عام.

من المرجح أن يحاول SQUAB SPIDER سرقة البيانات المتعلقة بالمعاملات من الضحايا.

التوقعات

على الرغم من أن حملات BGH الانتهازية تظل التهديد الأساسي للجرائم الإلكترونية في جميع القطاعات، فمن المرجح أن تستمر مجموعة فرعية أصغر من الجهات الفاعلة في الجرائم الإلكترونية في حملات الجرائم الإلكترونية المستهدفة التي تسعى إلى سرقة بيانات بطاقات الدفع أو المعاملات من الضحايا. وكما هو الحال مع نظام BGH البيئي، من المرجح أن تظل أدوات RMM المشروعة شائعة بين عمليات الجرائم الإلكترونية المستهدفة بسبب استخدامها على نطاق واسع في العمليات التجارية العادية. يسلط صمود الخصوم الذين يركزون على أمريكا اللاتينية SQUAB SPIDER وROBOT SPIDER وODYSSEY SPIDER وBLIND SPIDER الضوء على كيف من المرجح أن يستمر نظام الجرائم الإلكترونية المستهدف في أمريكا اللاتينية في الأمد المتوسط.



خاتمة

على مدار عام 2023، لاحظ CrowdStrike CAO أن الخصوم في جميع مجالات الاختراق المستهدف والجرائم الإلكترونية والقرصنة الإلكترونية يعملون بسرية غير مسبوقة. تظل القدرة على العمل دون أن يتم اكتشافها ذات أهمية قصوى بالنسبة للجهات الخبيثة، ويواصل مجرمو الإنترنت المتطورون اليوم اكتشاف أساليب جديدة لزيادة الفعالية وتحسين العمليات وتحقيق الأهداف.

ظلت الجرائم الإلكترونية تشكل حجر الزاوية في مشهد التهديدات في عام 2023، حيث كان خصوم SCATERED SPIDER وGRACEFUL SPIDER، BGH، مسؤولين عن معظم النشاط.

تقدر شركة CrowdStrike CAO أن BGH ستظل تشكل التهديد المهيمن في مشهد الجرائم الإلكترونية في عام 2024. تم إجراء هذا التقييم بثقة عالية بناءً على النجاح المستمر لهذه العمليات، كما هو موضح في النمو بنسبة 76٪ في وظائف DLS في عام 2023. تشمل الاتجاهات التي من المرجح ملاحظتها في عام 2024 لدعم عمليات BGH عمليات تسريب البيانات الخالية من برامج الفدية وزيادة العمليات التي تركز على السحابة.

استمر عدد الجهات الفاعلة التي تستهدف التهديدات التي تعتمد على الحوسبة السحابية في النمو في عام 2023 - كما في عام 2022 - ومن المرجح أن يستمر في النمو في عام 2024. إن الخصوم لديهم دافع كبير للاستثمار في الحوسبة السحابية وغيرها من التقنيات الجديدة واستخدامها، مثل الذكاء الاصطناعي التوليدي، لزيادة كفاءة ونجاح عملياتهم. سيسعى الخصوم الذين يعتمدون على الحوسبة السحابية إلى اكتشاف البيئات السحابية وحصرها والتنقل فيها لجمع معلومات ملكية قيمة من SharePoint وMicrosoft 365 ومستودعات التعليمات البرمجية. سيستخدمون هذه المعلومات في العمليات الجارية ومفاوضات الفدية أو ببساطة بيعها لخصوم آخرين في الجرائم الإلكترونية.

كما أدرك الخصوم ذوو الدوافع المالية بشكل متزايد فوائد العلاقات المخصصة في عام 2023، ومن المرجح أنهم تمكنوا من زيادة معدلات النجاح التشغيلي الناتجة. ومن المرجح أن يستمر وسطاء الوصول والجهات الفاعلة في RaaS في تكوين علاقات مخصصة في عام 2024. ومن المرجح أيضًا أن يتضمن العام المقبل تحسينات في فعالية الهندسة الاجتماعية وتجاوز MFA واستهداف مقدمي الخدمات من جهات خارجية في الجهود الرامية إلى الاستفادة من نقطة وصول واحدة أكبر.



لقد أدت الصراعات الجيوسياسية البارزة —وخاصة الصراع بين روسيا وأوكرانيا وإسرائيل وحماس —إلى استهداف كبير لعمليات الاختراق والنشاط الإلكتروني النشط في عام 2023، وخاصة بالنسبة للخصوم المرتبطين بإيران وروسيا. وفي عام 2024، سوف تظل هذه الصراعات البارزة وغيرها من الصراعات بمثابة محركات مهمة للنشاط الإلكتروني النشط.

وبعيداً عن النشاط السيبراني المرتبط بالصراع بين إسرائيل وحماس، ظل الخصوم المرتبطون بإيران مستمرين في استهداف منظمات الاتصالات، وهو الاتجاه الذي من المرجح أن يستمر في عام 2024. كما استمر الخصوم المرتبطون بروسيا في استهداف أوكرانيا وأعضاء حلف شمال الأطلسي والدول الشريكة. ومن المؤكد تقريباً أنهم سيستمرون في إجراء عمليات جمع المعلومات الاستخباراتية والتدخل في هذه المناطق الجغرافية في عام 2024.

قامت CrowdStrike CAO بتخريج العديد من مجموعات الأنشطة إلى خصوم معينين في عام 2023، بما في ذلك أول خصم على الإطلاق في مصر، WATCHFUL SPHINX.

وفقًا للتقييمات السابقة، تتوقع شركة CrowdStrike CAO أن تستمر غالبية الخصوم ومجموعات الأنشطة الراسخة في توسيع أو تحديث قدراتها في عام 2024. ومن المرجح أن يقوم عدد أقل من الخصوم ومجموعات الأنشطة في جميع أنحاء العالم بتوسيع نطاق أهدافهم المقدرة؛ وبدلاً من ذلك، من المرجح أن يستمروا في التركيز على مجموعات الأهداف التاريخية والإقليمية في الغالب.

في إطار مشهد تهديدات الثغرات الأمنية، يقدر CrowdStrike CAO أن العديد من اتجاهات عام 2023 - وهي استهداف الأجهزة الطرفية ومنتجات نهاية العمر التشغيلي - ستستمر في عام 2024. ظل مرتكبو جرائم الإنترنت يشكلون التهديد الأساسي لمعظم مستخدمي الأجهزة المحمولة في عام 2023 ومن المرجح أن يستمروا على هذا النحو في عام 2024. ومن المؤكد تقريبًا أن مرتكبي جرائم الاختراق المستهدفة سيستمرون في استهداف الأجهزة المحمولة، مع زيادة أمان النظام الأساسي والجهاز مما يتسبب في صعوبة عمل الخصوم الأقل تطورًا بنجاح في هذا المجال.

مع إنشاء Counter Adversary Operations، تظل CrowdStrike ثابتة في مهمتها لوقف الخروقات. من خلال الجمع بين أفضل المعلومات الاستخباراتية حول التهديدات وخدمة البحث عن التهديدات الاحترافية المُدارة التي لا مثيل لها في الصناعة، تضمن CrowdStrike لعملائها إمكانية الوصول إلى المعلومات الرائدة في الصناعة لتعزيز نجاحهم التشغيلي الفردي.

ظلت شركة CrowdStrike CAO تركز على تعطيل الخصم في عام 2023 وستستمر في تقديم معلومات استخباراتية لا مثيل لها حول التهديدات في عام 2024 وما بعده.

التوصيات

1

جعل حماية الهوية أمرا ضروريا

بسبب معدلات النجاح المرتفعة، ارتفعت وتيرة الهجمات القائمة على الهوية والهندسة الاجتماعية في عام 2023.
تمنح بيانات الاعتماد المسروقة الخصوم إمكانية الوصول والتحكم السريعين -وهي بوابة فورية للاختراق. لمواجهة هذه التهديدات، من الضروري تنفيذ مصادقة متعددة العوامل مقاومة للتصيد الاحتيالي وتوسيعها لتشمل الأنظمة والبروتوكولات القديمة، وتثقيف الفرق حول الهندسة الاجتماعية وتنفيذ التكنولوجيا التي يمكنها اكتشاف التهديدات وربطها عبر بيئات الهوية ونقطة النهاية والسحابة. تتيح الرؤية عبر النطاقات وتنفيذها لفرق الأمن اكتشاف الحركة الجانبية والحصول على رؤية كاملة لمسار الهجوم والبحث عن الاستخدام الضار

من الأدوات المشروعة. معالجة أساليب الوصول المعقدة مثل تبديل بطاقة SIM،
يتطلب تجاوز MFA وسرقة مفاتيح API وملفات تعريف الارتباط للجلسة وتذاكر Kerberos
الملاحقة الاستباقية والمستمرة للسلوكيات الضارة.

2

إعطاء الأولوية لمنصات حماية التطبيقات السحابية الأصلية (CNAPPs)

يشهد تبني الحوسبة السحابية نموًا هائلاً مع إدراك الشركات لإمكانات الابتكار
المرونة التجارية التي توفرها السحابة. وبسبب هذا النمو، أصبحت السحابة بسرعة
تعد السحابة ساحة معركة رئيسية للهجمات الإلكترونية. تحتاج الشركات إلى رؤية كاملة للسحابة، بما في ذلك التطبيقات وواجهات برمجة التطبيقات، للقضاء على التكوينات الخاطئة والثغرات الأمنية وغيرها من التهديدات الأمنية.
تعتبر أدوات أمان السحابة CNAPP بالغة الأهمية: لا ينبغي أن توجد أدوات أمان السحابة بمعزل عن غيرها، وتوفر أدوات أمان السحابة CNAPP منصة موحدة تبسط مراقبة التهديدات والثغرات الأمنية السحابية المحتملة واكتشافها والتصرف حيالها. حدد أداة أمان السحابة CNAPP التي تتضمن الحماية قبل وقت التشغيل والحماية أثناء التشغيل وتقنية بدون وكيل لمساعدتك في اكتشاف تطبيقاتك وواجهات برمجة التطبيقات التي تعمل في الإنتاج ورسم خريطة لها، مع إظهار جميع أسطح الهجوم والتهديدات والمخاطر التجارية الحرجة.

3

احصل على رؤية واضحة في المجالات الأكثر أهمية لمخاطر المؤسسة

غالبًا ما يستخدم الخصوم بيانات اعتماد صالحة للوصول إلى بيئات الضحايا التي تواجه السحابة ثم يستخدمون أدوات مشروعة لتنفيذ هجومهم، مما يجعل من الصعب على المدافعين التمييز بين نشاط المستخدم العادي والاختراق. لتحديد هذا النوع من الهجوم، تحتاج إلى فهم العلاقة بين الهوية والسحابة ونقطة النهاية وقياس حماية البيانات، والتي قد تكون في أنظمة منفصلة. في الواقع، تستخدم المؤسسة المتوسطة أكثر من 45 أداة أمان، مما يؤدي إلى إنشاء صوامع بيانات وفجوات في الرؤية. من خلال الدمج في منصة أمان موحدة مع قدرات الذكاء الاصطناعي، تتمتع المؤسسات برؤية كاملة في مكان واحد ويمكنها التحكم في عملياتها بسهولة. من خلال منصة أمان موحدة، توفر المؤسسات الوقت والمال ويمكنها اكتشاف وتحديد وإيقاف الخروقات بسرعة وثقة.

4

كفاءة القيادة: الخصوم هم تصبح أسرع - هل أنت كذلك؟

يستغرق الأمر من الخصوم 62 دقيقة في المتوسط - وأسرعها دقيقتين فقط - للانتقال أفقيًا من مضيف مخترق في البداية إلى مضيف آخر داخل البيئة. هل يمكنك مواكبة ذلك؟ دعنا نواجه الأمر - فشلت حلول SIEM القديمة في SOC. إنها بطيئة للغاية ومعقدة ومكلفة، وقد تم تصميمها لعصر كانت فيه أحجام البيانات - وسرعة وتعقيد الخصوم - جزءًا ضئيلًا مما هي عليه اليوم. أنت بحاجة إلى أداة أسرع وأسهل في النشر وأكثر فعالية من حيث التكلفة من حلول SIEM القديمة. ابحث عن طرق أفضل، مثل CrowdStrike Falcon® Next-Gen SIEM، الذي يوحد جميع عمليات اكتشاف التهديدات والتحقيق فيها والاستجابة لها في منصة واحدة تعتمد على الذكاء الاصطناعي ومقدمة عبر السحابة لتحقيق كفاءة وسرعة لا مثيل لها. أو إذا لم يكن لديك فريق مركز عمليات أمنية داخلي، ففكر في الاكتشاف والاستجابة المُدارة (MDR) على مدار الساعة طوال أيام الأسبوع.

5

بناء ثقافة الأمن السيبراني

على الرغم من أن التكنولوجيا تشكل أهمية بالغة في مكافحة الاختراقات ووقفها، إلا أن المستخدم النهائي يظل حلقة وصل حاسمة في سلسلة منع الاختراقات. ولابد من إطلاق برامج توعية المستخدمين لمكافحة التهديد المستمر المتمثل في التصيد الاحتيالي وتقنيات الهندسة الاجتماعية ذات الصلة. وبالنسبة لفرق الأمن، فإن الممارسة تؤدي إلى الكمال. لذا، شجع على إيجاد بيئة تقوم بشكل روتيني بإجراء تمارين على الطاولة وتشكيل فرق عمل لتحديد الثغرات والقضاء على نقاط الضعف في ممارسات الأمن السيبراني والاستجابة لها.

كراود سترايك المنتجات و خدمات

أمان نقطة النهاية

FALCON PREVENT | الجيل القادم من برامج مكافحة الفيروسات

يوفر الحماية ضد جميع أنواع التهديدات، من البرامج الضارة وبرامج الفدية إلى الهجمات المعقدة، ويتم نشره في دقائق، مما يحمي نقاط النهاية الخاصة بك على الفور

FALCON INSIGHT XDR | الكشف والاستجابة نقطة النهاية وما بعدها

تقدم EDR موحدة رائدة في الصناعة واكتشاف واستجابة ممتدة (XDR) مع رؤية على مستوى المؤسسة للكشف تلقائيًا عن نشاط الخصم والاستجابة عبر نقاط النهاية وجميع أسطح الهجوم الرئيسية

FALCON COMPLETE | الكشف والاستجابة المُدارة

يوقف التهديدات ويقضي عليها في دقائق مع إدارة الخبراء على مدار الساعة طوال أيام الأسبوع، والمراقبة والإصلاح الجراحي، والبحث الاستباقي عن التهديدات، واستخبارات التهديدات المتكاملة - كل ذلك مدعوم بأقوى ضمان لمنع الاختراق في الصناعة

FALCON COMPLETE XDR | الكشف الموسع المُدار و الاستجابة (MXDR)

توسيع خدمة MDR الرائدة في الصناعة من Falcon Complete من خلال حماية XDR عبر النطاقات التي تديرها خبرة CrowdStrike المتميزة على مدار الساعة طوال أيام الأسبوع، والبحث الاستباقي عن التهديدات وذكاء التهديدات الأصلي

إدارة جدار الحماية | FALCON جدار حماية المضيف

يوفر إدارة بسيطة ومركزية لجدار الحماية المضيف، مما يجعل من السهل إدارة سياسات جدار الحماية المضيف والتحكم فيها

التحكم في جهاز | FALCON أمان USB

يوفر الرؤية والتحكم الدقيق المطلوبين لتمكين الاستخدام الآمن لأجهزة USB في مؤسستك

FALCON للأجهزة المحمولة | اكتشاف نقاط النهاية والاستجابة لها

يوفر الحماية ضد التهديدات التي تتعرض لها أجهزة Android، وiOS ويوسع قدرات XDR/EDR إلى أجهزتك المحمولة، مع حماية متقدمة من التهديدات ورؤية في الوقت الفعلي للتطبيق ونشاط الشبكة

عمليات مكافحة الخصوم

فالكون أدفيرساري أوفرواتش MT | البحث الموحد عن التهديدات

يوفر حماية على مدار الساعة عبر نقاط النهاية والهوية وأحمال العمل السحابية التي يقدمها خبراء البحث عن التهديدات المدعومون بالذكاء الاصطناعي، ويتضمن معلومات استخباراتية مدمجة عن التهديدات لكشف ممارسات الخصم والثغرات الأمنية وبيانات الاعتماد المسروقة

استخبارات العدو من FALCON | أتمتة SOC

يقلل وقت الاستجابة من أيام إلى دقائق عبر مجموعة الأمان بأكملها من خلال أتمتة الاستخبارات الشاملة، ويمكّنك من إرسال التهديدات المحتملة على الفور إلى صندوق حماية آلي، واستخراج مؤشرات الاختراق ونشر التدابير المضادة - كل ذلك أثناء المراقبة المستمرة للاحتيال وحماية علامتك التجارية وموظفيك

والبيانات الحساسة

صائد الخصوم الصقر | مطاردة التهديدات بقيادة الاستخبارات

يوفر تقارير استخباراتية من الطراز العالمي، وتحليلات فنية، ومكتبات لتعقب التهديدات واكتشافها، ويختصر الوقت والتكلفة اللازمين لفهم والدفاع ضد خصوم الدولة القومية المتطورة والجرائم الإلكترونية والقراصنة الإلكترونيين

عمليات مكافحة الخصوم من طراز فالكون النخبة

محلل حسب الطلب

توفير محلل مخصص يستخدم أدوات متقدمة للتحقيق والبحث عن التهديدات مدعومة بمعلومات استخباراتية عميقة عن الخصوم لتحديد وتعطيل الخصوم عبر بيئة تكنولوجيا المعلومات الخاصة بك وخارجها

أمن السحابة

فالكون للأمن السحابي

يوفر حماية من الاختراق، بما في ذلك استخبارات التهديدات والكشف عنها والاستجابة لها؛ وحماية وقت تشغيل عبء العمل؛ وإدارة وضع أمان السحابة عبر Google وAzure وAWS
منصة السحابة (GCP)

FALCON CLOUD SECURITY للأمن السحابي للحاويات

يوفر أمان السحابة والحاويات وحماية الاختراق؛ وإدارة وضع أمان السحابة؛ واكتشاف التهديدات والاستجابة لها عبر البيئات المحلية والهجينة ومتعددة السحابات؛ وحماية أحمال العمل السحابية، بما في ذلك أمان الحاويات وحماية Kubernetes

FALCON CLOUD SECURITY للحاويات المُدارة

يوفر أمان السحابة والحاويات، بما في ذلك استخبارات التهديدات والكشف عنها والاستجابة لها؛ وأمان صور الحاويات؛ وحماية Kubernetes

FALCON OVERWATCH - مطاردة التهديدات السحابية

الخدمات المُدارة

يكشف عن تهديدات السحابة، بدءًا من مسارات هجوم السحابة الفريدة مع مسارات معقدة من عمليات إدخال وإخراج السحابة ومؤشرات سوء التكوين (IOMs)
إلى نشاط الخصم المخفي جيدًا في البنية الأساسية السحابية الهامة لديك —بما في ذلك AWS وAzure وGCP

فالكون للأمن السحابي الكامل

MDR لأحمال العمل السحابية

توفر خدمة حماية أحمال العمل السحابية المُدارة بالكامل، وتوفر إدارة أمنية متخصصة على مدار الساعة طوال أيام الأسبوع، ومطاردة التهديدات،
والمراقبة والاستجابة لأحمال العمل السحابية، بدعم من
ضمان منع الاختراق الرائد في الصناعة من CrowdStrike

حماية الهوية

الكشف عن تهديدات الهوية من خلال FALCON

يتيح الكشف الدقيق عن التهديدات القائمة على الهوية في الوقت الفعلي، والاستفادة من الذكاء الاصطناعي والتحليلات السلوكية لتوفير رؤى عملية عميقة
لوقف الهجمات الحديثة مثل
برامج الفدية

حماية الهوية من التهديدات من خلال FALCON

يتيح اكتشاف التهديدات بدقة فائقة والوقاية في الوقت الفعلي من الهجمات القائمة على الهوية من خلال الجمع بين قوة الذكاء الاصطناعي المتقدم والتحليلات
السلوكية ومحرك السياسة المرن لفرض الوصول المشروط القائم على المخاطر

برنامج FALCON لحماية الهوية من التهديدات

حماية الهوية من التهديدات المُدارة

يوفر حلاً كاملاً لإدارة حماية الهوية يوفر الوقاية من التهديدات المتعلقة بالهوية في الوقت الفعلي وإنفاذ سياسات تكنولوجيا المعلومات ومراقبتها وإصلاحها
-مدعومًا على مدار الساعة طوال أيام الأسبوع من قبل فريق خبراء CrowdStrike

العمليات الأمنية وتكنولوجيا المعلومات

فالكون ديسكوفر | تكنولوجيا المعلومات النظافة

يحدد الحسابات والأنظمة والتطبيقات غير المصرح بها في أي مكان في بيئتك في الوقت الفعلي، مما يتيح الرؤية الفورية لتحسين وضعك الأمني العام

FALCON SPOTLIGHT | إدارة الثغرات الأمنية

يقدم لفرق الأمان حلاً شاملاً وآليًا لإدارة الثغرات الأمنية، مما يتيح تحديد الأولويات بشكل أسرع وتدفقات عمل متكاملة للإصلاح دون الحاجة إلى عمليات مسح كثيفة الموارد

إدارة التعرض للصقر | إدارة التعرض

يتيح لفرق الأمن تحديد أولويات التعرضات التي تحدث أكبر تأثير وتقليل فرصة الخصم للاختراق والحركة الجانبية بشكل استباقي

فالكون سيرفيس | إدارة الهجوم الخارجي على السطح

يكتشف ويرسم باستمرار جميع الأصول التي تواجه الإنترنت لإغلاق التعرض المحتمل من خلال خطط التخفيف الموجهة لتقليل سطح الهجوم

حماية البيانات من شركة فالكون | حماية البيانات الموحدة

يوفر رؤية عميقة في الوقت الفعلي لما يحدث مع البيانات الحساسة ويوقف سرقة البيانات من خلال فرض السياسات التي تتبع المحتوى تلقائيًا وليس الملفات

FALCON FILEVANTAGE | مراقبة سلامة الملفات

يوفر رؤية شاملة ومركزية في الوقت الفعلي تعمل على تعزيز الامتثال وتقديم بيانات سياقية ذات صلة

فالكون فورنسيكس | الأمن السيبراني الجنائي

يقوم بأتمتة جمع بيانات الفرز الجنائي في وقت معين وتاريخي لتحليل قوي لحوادث الأمن السيبراني

FALCON FOR IT | سير العمل الآلي

توسيع منصة Falcon لأتمتة سير عمل تكنولوجيا المعلومات والأمان من خلال دورة حياة شاملة من الرؤية إلى العمل

الجيل القادم من SIEM

FALCON NEXT-GEN SIEM | إدارة SIEM والسجلات

يتيح لك إغلاق الخصوم بسرعة وخفض تكاليف مركز العمليات الأمنية من خلال توحيد الكشف الرائد في الصناعة والاستخبارات من الطراز العالمي والبحث السريع والتحقيقات التي يقودها الذكاء الاصطناعي في منصة واحدة مقدمة عبر السحابة

خدمات كراود سترايك

الاستجابة للحوادث

أوقف الخروقات النشطة وأعد النظام باستخدام أكثر الأشخاص علمًا وكفاءة

فريق العلاقات مع المستثمرين متاح

الاستجابة للحوادث

تقييم التسوية

استعادة نقطة النهاية

خدمات اكتشاف الشبكة

خدمات الاحتفاظ

الخدمات الاستشارية الاستراتيجية

تطوير برنامج الأمان وتحسينه لتحسين الدفاعات

- تمارين الطاولة
- تقييم النضج
- تقييم الدفاع ضد برامج الفدية
- تقييم SOC
- استعدادات لجنة الأوراق المالية والبورصات
- إحاطات مجلس الإدارة والمدير التنفيذي

خدمات الفريق الأحمر

اختبار الإجهاد والتحقق من صحة الدفاعات من خلال الهجمات المحاكاة

- اختبار الاختراق
- تمرين الفريق الأحمر/الفريق الأزرق
- تمرين محاكاة الخصم

خدمات السحابة والهوية

تأمين المحيط الجديد بشكل استباقي

- تقييم أمن الهوية
- تقييم أمن السحابة
- تمرين الفريق الأحمر/الفريق الأزرق للسحابة
- تقييم الاختراق السحابي

الخدمات الاستشارية الفنية

التدقيق على الثغرات الأمنية ومعالجتها لتقليل المخاطر بشكل ملموس

- تقييم المخاطر الفنية
- تقييم مخاطر التهديدات السيبرانية

التدريب وتطوير المهارات الأمنية

كن خبيرًا أمنيًا تحت وصاية CrowdStrike

Machine Translated by Google



عن
كراود سترايك

أعادت شركة CrowdStrike (المدرجة في بورصة ناسداك تحت الرمز CRWD)، الرائدة عالمياً في مجال الأمن السيبراني، تعريف الأمن الحديث من خلال منصة السحابة الأكثر تقدماً في العالم لحماية المجالات الحرجة لمخاطر المؤسسة - نقاط النهاية وأحمال العمل السحابية والهوية والبيانات.

بفضل CrowdStrike Security Cloud والذكاء الاصطناعي من الطراز العالمي، تستفيد منصة CrowdStrike Falcon® من مؤشرات الهجوم في الوقت الفعلي واستخبارات التهديد والمهارات التجارية المتطورة للعدو والقياس عن بعد المثري من جميع أنحاء المؤسسة لتقديم اكتشافات فائقة الدقة والحماية الآلية والعلاج وصيد التهديدات النخبوية وإمكانية مراقبة نقاط الضعف ذات الأولوية.

تم تصميم منصة Falcon خصيصًا في السحابة باستخدام بنية وكيل خفيفة الوزن واحدة، وتوفر نشرًا سريعًا وقابلًا للتطوير وحماية وأداءً فائقين وتعقيدًا أقل ووقتًا فوريًا للحصول على القيمة.

CrowdStrike: نوقف الخروقات.

لمعرفة المزيد: www.crowdstrike.com

تابعونا: المدونة | س | لينكدإن | فيسبوك | انستجرام

ابدأ تجربة مجانية اليوم: www.crowdstrike.com/free-trial-guide


2024
GLOBAL THREAT REPORT
CROWDSTRIKE

Foreword

The 2024 edition of the CrowdStrike Global Threat Report arrives at a pivotal moment for our global community of protectors. The speed and ferocity of cyberattacks continue to accelerate as adversaries compress the time between initial entry, lateral movement and breach. At the same time, the rise of generative AI has the potential to lower the barrier of entry for low-skilled adversaries, making it easier to launch attacks that are more sophisticated and state of the art.

These trends are driving a tectonic shift in the security landscape and the world. The “good enough” approach to cybersecurity is simply no longer good enough for modern threats. As organizations increasingly move business to the cloud, adversaries are advancing their capabilities to exploit this, and abuse features unique to the cloud. We continue to see identity-based attacks take center stage, as adversaries focus on social engineering attacks that bypass multifactor authentication. The use of legitimate tools to execute an attack, an increasingly prevalent technique, impedes the ability to differentiate between normal activity and a breach.

We are entering an era of a cyber arms race where AI will amplify the impact for both the security professional and the adversary. Organizations cannot afford to fall behind, and the legacy technology of yesterday is no match for the speed and sophistication of the modern adversary.

With the release of the CrowdStrike 2024 Global Threat Report, our elite Counter Adversary Operations team is delivering the actionable intelligence you need to stay ahead of today’s threats and secure your future. This year’s report provides critical insight and observations into adversary activity, including:

- The tactics and techniques that adversaries use to exploit gaps in cloud protection
- The continued exploitation of stolen identity credentials and increasingly sophisticated methods adversaries use to gain initial access
- The growing menace of supply chain attacks and exploitation of trusted software to maximize the ROI of attacks
- The potential for adversaries to target global elections in a year that has the potential to transform geopolitics around the world for the near future

From Day One, CrowdStrike has said, “You don’t have a malware problem, you have an adversary problem.” We pioneered the concept of adversary-focused cybersecurity because it’s the best way to protect customers and stop breaches. We know the adversary better than anyone, and we use this insight to guide our innovation, protect customers, stop breaches and increase the cost to the adversary.

A secure future requires a strong foundation. This is what we’re delivering with the AI-native CrowdStrike Falcon® XDR platform. We’re driving the convergence of data, cybersecurity and IT, with generative AI and workflow automation built natively within a single, unified platform to give you and your teams the speed you need to beat the adversary.

I hope you find the CrowdStrike 2024 Global Threat Report informative and inspiring in our shared fight against the adversary. CrowdStrike will remain unrelenting in our mission to deliver the security outcome you need most: stopping the breach.

George Kurtz

George Kurtz
CrowdStrike CEO/Co-Founder

Table of Contents



Introduction

As we reflect on the 2023 cyber threat landscape, the theme of stealth prevails. Adversaries have faced a hardening attack surface thanks to advancements in threat defense technology and threat awareness, and they have responded by increasingly adopting and relying on techniques that empower them to move faster and evade detection.

These techniques are evident in the consistent prevalence of eCrime, a highly attractive and lucrative business venture for many criminals. Unsurprisingly, eCrime persisted as the most pervasive threat across the 2023 threat landscape as adversaries leveraged techniques to maximize stealth, speed and impact.

While ransomware remains the tool of choice for many big game hunting (BGH) adversaries, data-theft extortion continues to be an attractive — and often easier — monetization route, as evidenced by the 76% increase in the number of victims named on BGH dedicated leak sites (DLSs) between 2022 and 2023. Access brokers continued to profit by providing initial access to eCrime threat actors throughout the year, with the number of advertised accesses increasing by 20% from 2022.

Nation-state adversaries were also active throughout 2023. China-nexus adversaries continued to operate at an unmatched pace across the global landscape, leveraging stealth and scale to collect targeted group surveillance data, strategic intelligence and intellectual property.

In other areas of the world, conflict continued to drive nation-state and hacktivist adversary activity. In 2023, as the Russia-Ukraine war entered its second year, Russia-nexus adversaries and activity clusters maintained high, sustained levels of activity in support of Russian Intelligence Service intelligence collection, disruptive activity, and information operations (IO) targeting Ukraine and NATO countries.

>>

DATA-THEFT EXTORTION CONTINUES TO BE AN ATTRACTIVE — AND OFTEN EASIER — MONETIZATION ROUTE, AS EVIDENCED BY THE 76% INCREASE IN THE NUMBER OF VICTIMS NAMED ON BGH DEDICATED LEAK SITES



Iran-nexus adversaries and Middle East hacktivist adversaries were also observed pivoting cyber operations in the latter half of the year in alignment with kinetic operations stemming from the 2023 Israel-Hamas conflict.

North Korean adversaries maintained a consistently high tempo throughout 2023. Their activity continued to focus on financial gain via cryptocurrency theft and intelligence collection from South Korean and Western organizations, specifically in the academic, aerospace, defense, government, manufacturing, media and technology sectors.

Across the rest of the world, stealth played a key role in adversary activity focused on digital surveillance, information collection and control in support of government agendas. The assessed geographic range of this activity, as well as the capabilities and target scope of global threat actors, continued to underscore the extent to which targeted intrusion capabilities have proliferated beyond those demonstrated by commonly reported countries. In some cases, this activity was assisted by private sector offensive actors and openly available adversary emulation frameworks.

One of the greatest threat actor motivations driving stealth in cyber threat operations is CrowdStrike's development of new products and partnerships throughout 2023. These changed the stakes within the operational landscape and left adversaries with no place to hide.

In 2023, CrowdStrike Falcon® Intelligence and CrowdStrike® Falcon OverWatch™ merged to become CrowdStrike Counter Adversary Operations (CAO). Combining the power of threat intelligence with the speed of dedicated hunting teams and trillions of cutting-edge telemetry events from the AI-native CrowdStrike Falcon® platform that detect, disrupt and stop today's sophisticated adversaries, this merger has exponentially raised the business cost of conducting cyberattacks. In 2024, CrowdStrike CAO repackaged CrowdStrike's threat intelligence modules to add managed threat hunting (an industry first), empowering organizations to better pursue adversaries and stop breaches.

Over the course of 2023, CrowdStrike CAO introduced 34 new adversaries — including a newly tracked, Egypt-based adversary, WATCHFUL SPHINX — raising the total number of actors tracked across all motivations to 232. In addition to named adversaries, CrowdStrike CAO tracks more than 130 active malicious activity clusters.

CrowdStrike CAO drives unparalleled, actionable reporting coverage that captures new cyber threat developments in real time and identifies and tracks new adversaries. The CrowdStrike 2024 Global Threat Report sheds light on the standout trends from last year, how adversaries' activities and motivations are evolving and the ways CrowdStrike anticipates the threat landscape will evolve in the coming year.

OVER THE COURSE OF 2023, CROWDSTRIKE CAO INTRODUCED 34 NEW ADVERSARIES – INCLUDING A NEWLY TRACKED, EGYPT-BASED ADVERSARY, WATCHFUL SPHINX – RAISING THE TOTAL NUMBER OF ACTORS TRACKED ACROSS ALL MOTIVATIONS TO 232.
IN ADDITION TO NAMED ADVERSARIES, CROWDSTRIKE CAO TRACKS MORE THAN 130 ACTIVE MALICIOUS ACTIVITY CLUSTERS.



CrowdStrike CAO Innovations

THE CROWDSTRIKE CAO TEAM PUTS RAPID INSIGHTS INTO THE HANDS OF FRONT-LINE TEAMS SO THEY CAN DISRUPT ADVERSARIES FASTER THAN EVER BEFORE.

IN THE FALL OF 2023, CROWDSTRIKE CAO ROLLED OUT AN IDENTITY THREAT HUNTING CAPABILITY, PAIRING THE LATEST INTELLIGENCE ON ADVERSARY MOTIVES AND TACTICS, TECHNIQUES AND PROCEDURES (TTPS) WITH CROWDSTRIKE FALCON® IDENTITY THREAT PROTECTION AND ELITE CAO THREAT HUNTERS TO QUICKLY IDENTIFY AND REMEDIATE COMPROMISED CREDENTIALS, TRACK LATERAL MOVEMENT AND STAY AHEAD OF ADVERSARIES WITH 24/7 COVERAGE.

AND WHILE THE CAO TEAM HUNTS FOR ADVERSARY ACTIVITY INSIDE CUSTOMER ORGANIZATIONS, THE NEW CAO "EXTERNAL ATTACK SURFACE EXPLORE" CAPABILITY ENABLES CUSTOMERS TO HUNT FOR AND EXAMINE ADVERSARY INFRASTRUCTURE.

CROWDSTRIKE MADE KEY INVESTMENTS IN AUTOMATION IN 2023, HELPING CUSTOMERS IMMEDIATELY TAKE ACTION ON CAO-IDENTIFIED THREATS. VIA FALCON IDENTITY THREAT PROTECTION, CROWDSTRIKE INTRODUCED NEW AUTOMATED WORKFLOWS FOR RESETTING CUSTOMER PASSWORDS EXPOSED ON THE CRIMINAL UNDERGROUND; ONE-CLICK TYPOSQUATTING DOMAIN BLOCKING AND TAKEDOWN; AND NEW CROWDSTRIKE FALCON® FUSION PLAYBOOKS FOR AUTOMATIC INDICATORS OF COMPROMISE (IOCS) RESULTING FROM TYPOSQUATTING THREATS AND THIRD-PARTY SYSTEM INTEGRATION. THESE NEW ENHANCEMENTS ALLOW USERS TO QUICKLY RESPOND TO THREATS THROUGHOUT THEIR SECURITY WORKFLOWS.

THE NEW CROWDSTRIKE CAO MODULES — CROWDSTRIKE FALCON® ADVERSARY OVERWATCH™, CROWDSTRIKE FALCON® ADVERSARY INTELLIGENCE AND CROWDSTRIKE FALCON® ADVERSARY HUNTER — HAVE LINKED THREAT HUNTING EVEN MORE CLOSELY TO THEIR INTELLIGENCE CAPABILITIES, UNIFYING THE USER EXPERIENCE SO CUSTOMERS CAN EASILY LEVERAGE A SINGLE, CONSISTENT USER INTERFACE TO VIEW CRUCIAL INFORMATION ACROSS ALL CAO CAPABILITIES.

CROWDSTRIKE CUSTOMERS ALSO BENEFIT FROM ENHANCED CONTEXT AROUND OBSERVABLES, NEW INDICATOR OF ATTACK (IOA) INTEGRATIONS TO ACCELERATE SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DETECTION AND RESPONSE, THREAT HUNTING WORKFLOWS THAT WILL MORE EFFECTIVELY IDENTIFY ENVIRONMENTAL THREATS, AND IMPROVEMENTS TO DATA UNIFICATION AND LINKAGE ACROSS THE FALCON PLATFORM AND THIRD-PARTY APPLICATIONS.

NAMING CONVENTIONS

Adversary	Nation-State or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPHINX	EGYPT
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURKEY

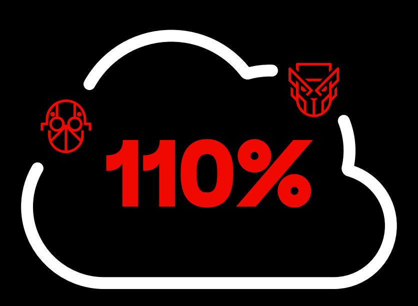


Threat Landscape Overview

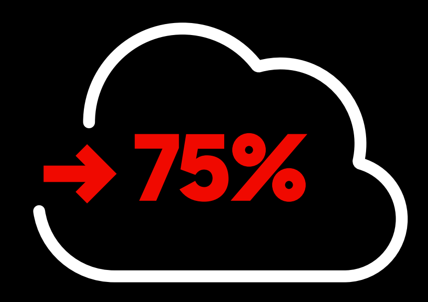
year over year = (YoY)



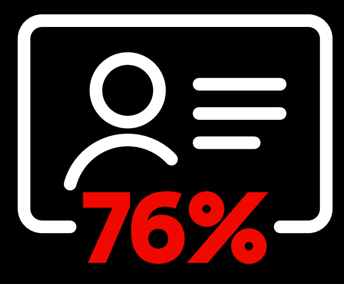
34 new adversaries tracked by CrowdStrike, raising the total to **232**



Cloud-conscious cases increased by **110% YoY**



Cloud environment intrusions increased by **75% YoY**



76% YoY increase in victims named on eCrime dedicated leak sites



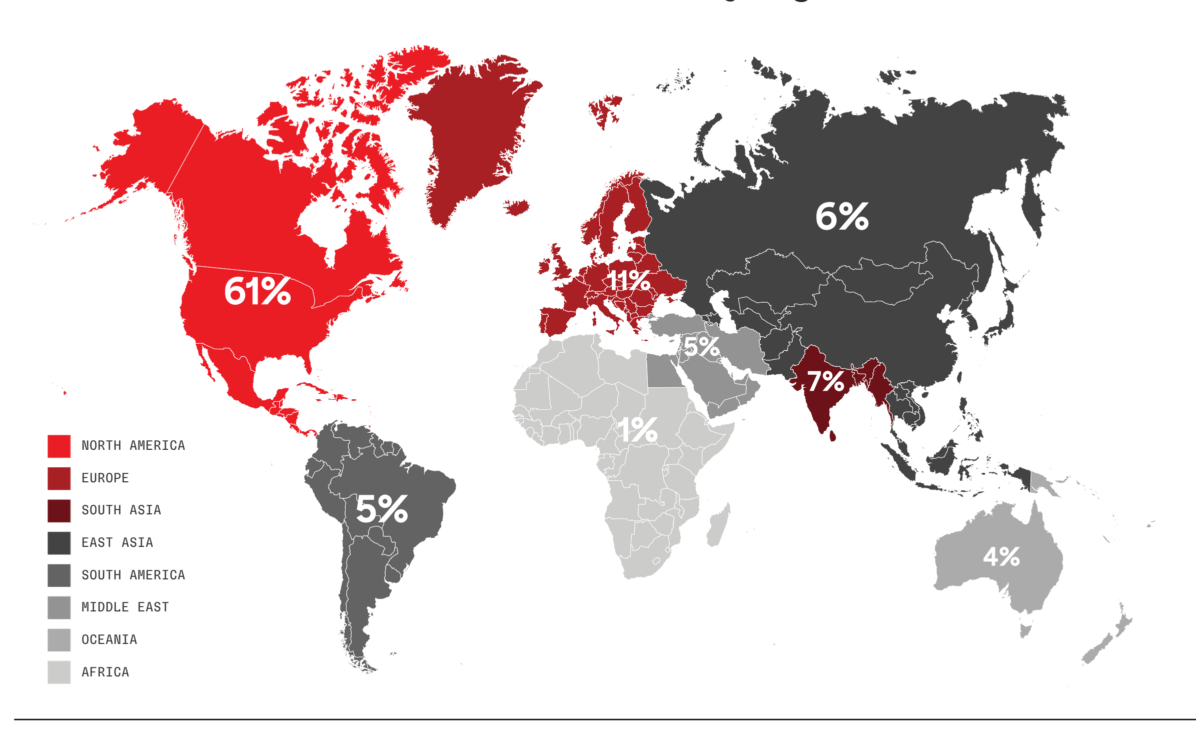
84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

Today's cyber threats are particularly alarming due to the widespread use of hands-on or "interactive intrusion" techniques, which involve adversaries actively executing actions on a host to accomplish their objectives. Unlike malware attacks that depend on the deployment of malicious tooling and scripts, interactive intrusions leverage the creativity and problem-solving skills of human adversaries. These individuals can mimic expected user and administrator behavior, making it difficult for defenders to differentiate between legitimate user activity and a cyberattack.

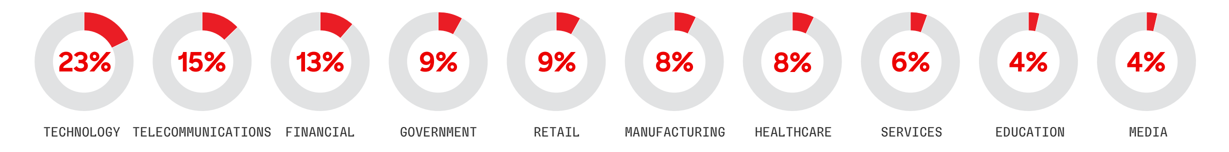
In 2023, CrowdStrike observed a 60% year-over-year increase in the number of interactive intrusion campaigns, with a 73% increase in the second half compared to 2022.

The technology sector was the most frequently targeted industry in which CrowdStrike CAO observed interactive intrusion activity in 2023, a continuing trend from 2022. The charts below reflect the relative frequency of intrusions in the top 10 industry verticals and in geographical regions.

Interactive Intrusions by Region



Interactive Intrusions by Industry

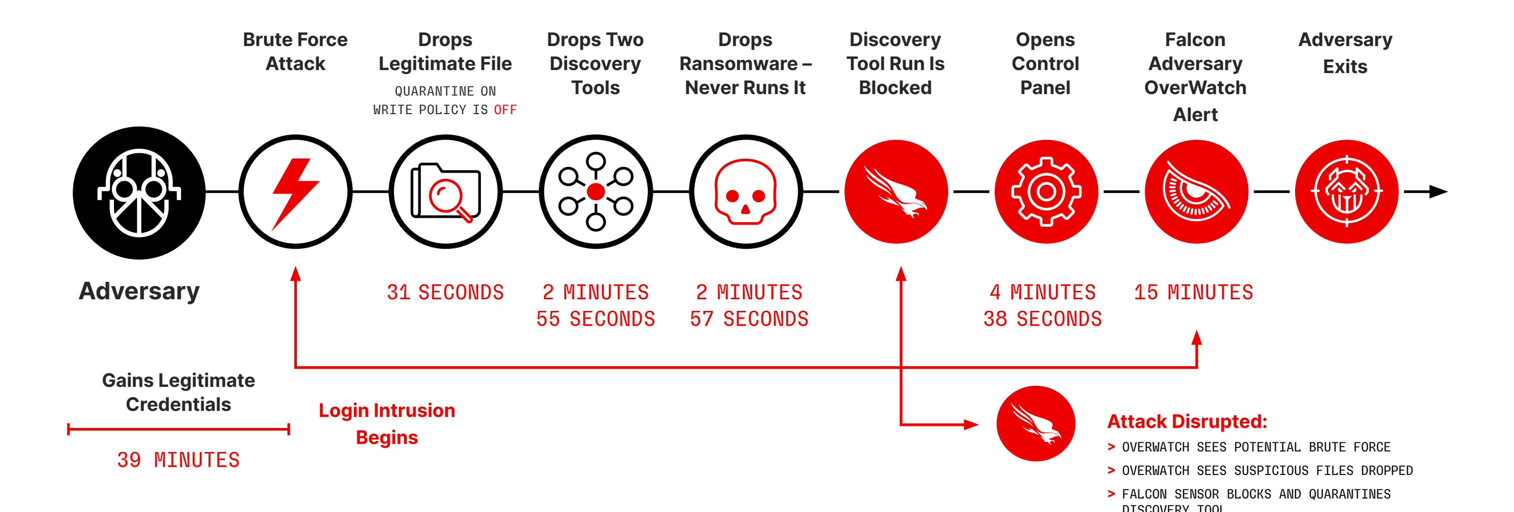


After gaining initial access to a network, adversaries seek to "break out" and move laterally from the compromised host to other hosts within the environment. The time it takes for them to do this — "breakout time" — is crucial because the initially compromised machines are rarely the ones adversaries need to achieve their goals. They must move laterally into the network, conduct reconnaissance, establish persistence and locate their targets. Responding within the breakout time window allows defenders to mitigate costs and other damages associated with intrusions.

This year, the average breakout time for interactive eCrime intrusion activity decreased from 84 minutes in 2022 to 62 minutes in 2023. The fastest observed breakout time was only 2 minutes and 7 seconds.

Anatomy of an eCrime Interactive Intrusion

To gain a better understanding of interactive intrusions, the following timeline illustrates the speed of a real-world hands-on attack:



Falcon Adversary OverWatch Response:
- HOST NETWORK ISOLATED
- PASSWORD RESET

In this case, the security team had the “quarantine on write” policy setting disabled, enabling the four files to be written to disk. The adversary executed a legitimate tool to obtain system information for reconnaissance and then dropped three more files, including ransomware, onto the system. They attempted to execute a network discovery and reconnaissance tool to map out lateral movement options, which was immediately blocked and quarantined by the Falcon sensor. This caused the adversary to open the control panel to understand which security tool was in use. When they identified the Falcon platform, they never attempted to execute the second discovery tool or the ransomware (which would have been prevented and quarantined) and moved to another victim. Within minutes, CrowdStrike CAO threat hunters notified the customer, took the machine offline and reset the user password.

Once an initial compromise occurs, it only takes seconds for adversaries to drop tools and/or malware on a victim’s environment during an interactive intrusion. However, the saying “time is money” holds true for adversaries. More than 88% of the attack time was dedicated to breaking in and gaining initial access. By reducing or eliminating this time, adversaries free up resources to conduct more attacks.

To do this, they have continued to move beyond malware to faster, more effective means such as identity attacks (phishing, social engineering and access brokers) and the exploitation of vulnerabilities and trusted relationships. This trend is apparent over the last five years, as malware-free activity represented 75% of detections in 2023 — up from 71% in 2022.

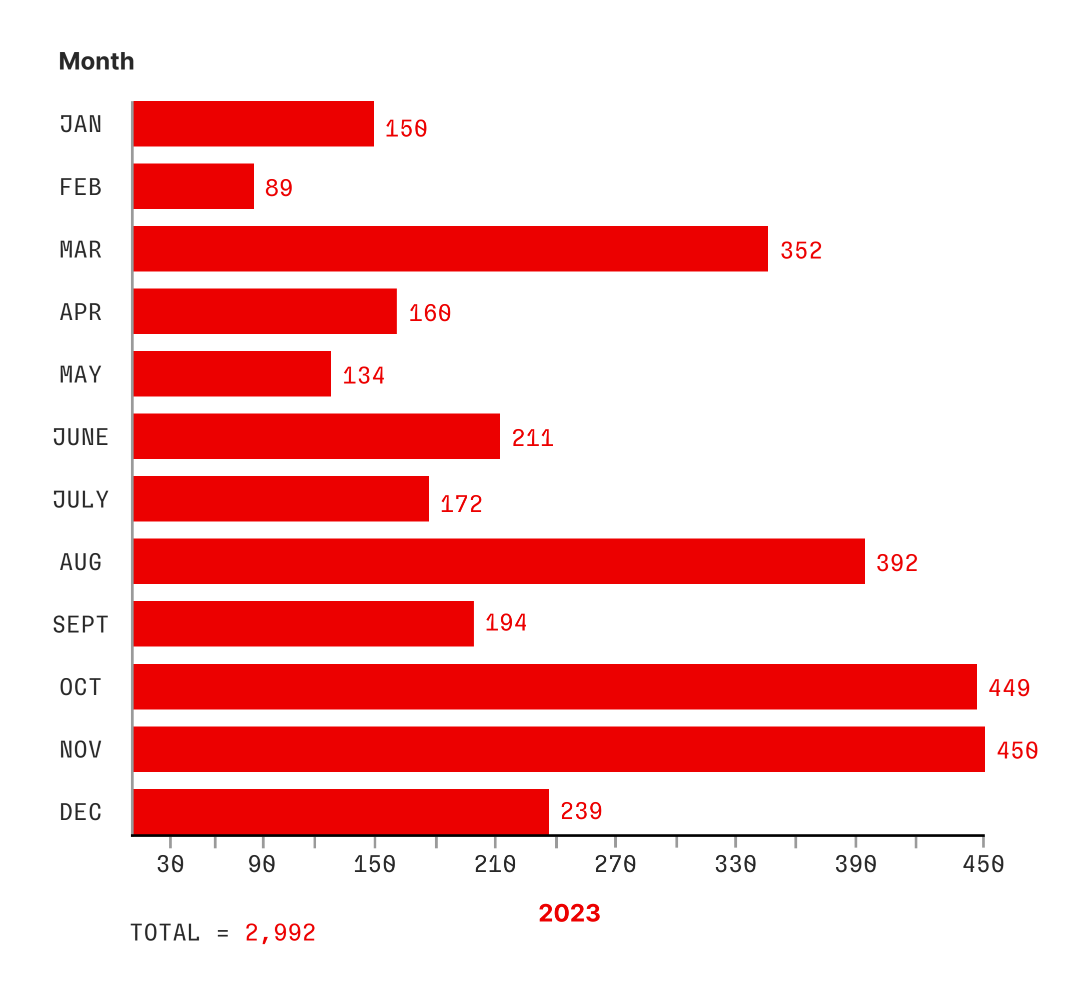
MALWARE-FREE ACTIVITY



75% 2023
71% 2022
62% 2021
51% 2020
40% 2019

This trend is partly related to the success of identity attacks, access brokers and the prolific abuse of valid credentials to facilitate access and persistence in victim environments. Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators. These adversaries continued to profit from providing initial access to a variety of eCrime threat actors in 2023, with the number of accesses advertised increasing by almost 20% compared to 2022.

Access Broker Advertisements by Month



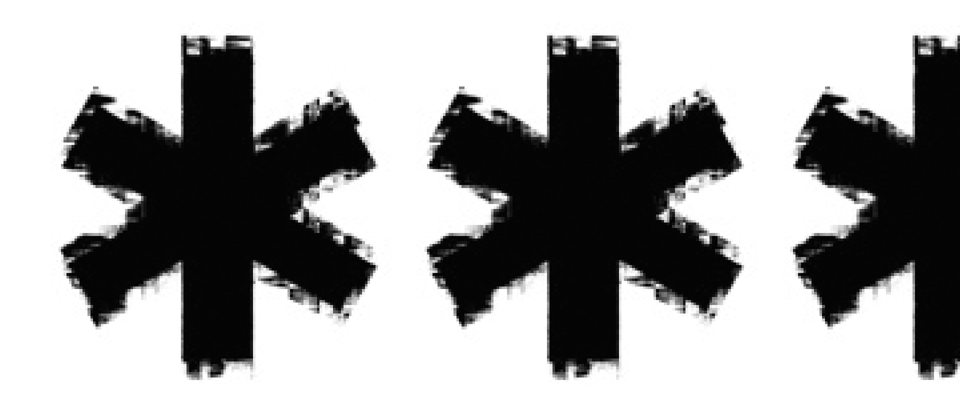
Today's sophisticated cyberattacks only take minutes to succeed. Adversaries use techniques such as interactive hands-on-keyboard attacks and legitimate tools to attempt to hide from detection. To further accelerate attack tempo, adversaries can access credentials in multiple ways, including purchasing them from access brokers for a few hundred dollars. Organizations must prioritize protecting identities in 2024.

2023 Themes

IDENTITY-BASED AND SOCIAL ENGINEERING ATTACKS

Adversaries spanning multiple motivations and regions continue to use phishing techniques spoofing legitimate users to target valid accounts, as well as other authentication and identifying data, to conduct their attacks. In addition to stealing account credentials, CrowdStrike CAO observed adversaries targeting API keys and secrets, session cookies and tokens, one-time passwords (OTPs) and Kerberos tickets throughout 2023.





ACCOUNT CREDENTIALS

Adversaries can authenticate to a system and/or user account using stolen credentials, which can either be obtained by the adversary directly (for example, using information stealers or exploiting unmanaged edge devices) or by purchasing them.

API KEYS AND SECRETS

Access to protected resources using stolen API keys and secrets may allow an adversary to steal sensitive data. Unless the API keys and secrets are changed, the adversary could maintain indefinite access.

SESSION COOKIES AND TOKENS

Adversaries can steal session cookies and tokens to masquerade as the legitimate user and authenticate to an application.

ONE-TIME PASSWORDS (OTPs)

OTP theft allows the adversary to bypass multifactor authentication (MFA) by SIM swapping, SS7 attacks, socially engineering the victim or email compromise.

KERBEROS AND KERBEROS TICKETS

By stealing or forging Kerberos tickets, adversaries can gain access to encrypted credentials, which can then be cracked offline. CrowdStrike CAO recorded a 583% increase in Kerberoasting attacks in 2023.

Figure 1. Identity-based attack vectors

BEAR Adversaries Conduct Credential Collection Campaigns

FANCY BEAR conducted regular credential collection campaigns throughout 2023. In March 2023, Microsoft patched a zero-day elevation-of-privilege vulnerability in Microsoft Outlook (CVE-2023-23397), which FANCY BEAR had been exploiting since at least March 2022 to solicit NT LAN Manager authentication sessions from targets using specially crafted spear-phishing emails. The Polish Cyber Command reported that the adversary used this authentication data to connect to Exchange servers and change additional high-value account mailbox permissions through the Exchange Web Services protocol.[1]

FANCY BEAR also conducted credential phishing campaigns and developed a custom toolkit to capture credentials from Yahoo! Mail and ukr.net webmail users. The adversary expanded this toolkit to use the Browser-in-the-Browser technique in April 2023 and added MFA interception capabilities to its toolkit to collect OTPs sent to the MFA contact (e.g., a phone number) linked to the targeted account.

COZY BEAR has conducted credential phishing campaigns using Microsoft Teams messages to solicit MFA tokens for Microsoft 365 accounts since at least late May 2023. If a user accepts its initial message request, COZY BEAR attempts to socially engineer the target by claiming a change was made to their current MFA settings and stating an MFA code is required for verification.

CrowdStrike® Services has observed COZY BEAR connecting to a compromised account using Microsoft Entra ID (previously Azure Active Directory) before registering a new device and enabling a passwordless phone sign-in for the user. The adversary also exported certificates containing private keys and requested a KRBTGT-authentication ticket for a different account using a legitimately issued certificate.



1 https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/



SCATTERED SPIDER Conducts Sophisticated Social Engineering Campaigns

Identity-based techniques are also central to SCATTERED SPIDER tradecraft. Throughout 2023, this adversary conducted sophisticated social engineering campaigns to access victim accounts. SCATTERED SPIDER's tactics included SMS phishing (smishing) and voice phishing (vishing) to harvest credentials and phone calls made to victim organization help desks to persuade support personnel to provide password and/or MFA resets for targeted accounts. In many cases, SCATTERED SPIDER also leveraged earlier intrusions at telecom organizations to SIM swap targeted employee phone numbers, enabling the adversary to then receive SMS messages containing OTP codes.

SCATTERED SPIDER deliberately selects social engineering campaign targets from employees in information security and other IT-related teams. This is likely due to direct employee access to security tools as well as applications and documentation that may support lateral movement and further account compromise. In a minority of incidents, SCATTERED SPIDER targeted accounts belonging to employees who had direct access to company financial resources.

Additionally, SCATTERED SPIDER often configured residential proxies to appear as though they were logging in to victim accounts from the same geographical area as the legitimate account owner. In doing so, the adversary further exhibited its understanding of identity-related security policies in enterprise organizations.

ADVERSARIES CONTINUE TO DEVELOP CLOUD-CONSCIOUSNESS

As predicted, cloud environment intrusions increased by 75% from 2022 to 2023 (Figure 2), with cloud-conscious cases increasing by 110% and cloud-agnostic cases increasing by 60%.

Cloud-conscious is a term referring to threat actors who are aware of the ability to compromise cloud workloads and use this knowledge to abuse features unique to the cloud for their own purposes.

eCrime adversaries are especially active in targeting cloud environments: 84% of cloud-conscious intrusions attributed to adversaries were conducted by likely eCrime actors, compared to 16% conducted by targeted intrusion actors. Traditional BGH adversaries, such as INDRIK SPIDER, became more cloud-conscious throughout the year.

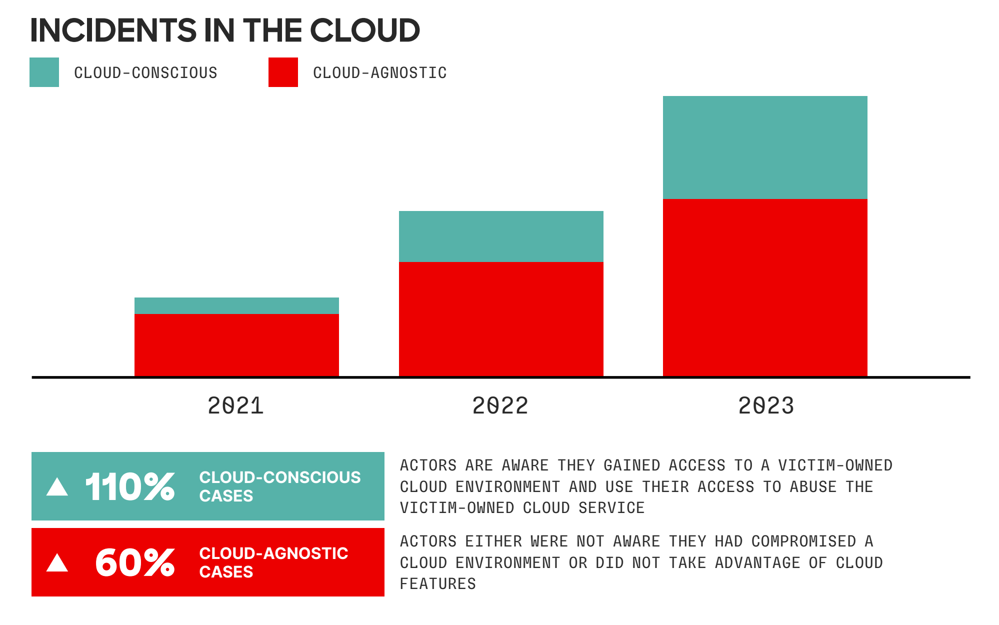


Figure 2. Increases in cloud cases

SCATTERED SPIDER predominantly drove cloud-conscious activity increases throughout 2023, accounting for 29% of total cases. Throughout 2023, SCATTERED SPIDER demonstrated progressive and sophisticated tradecraft within targeted cloud environments to maintain persistence, obtain credentials, move laterally and exfiltrate data.

Adversaries' preference for identity-based techniques is evident in their cloud-focused attacks. Next are several observations of cloud- and identity-focused activities categorized by the MITRE ATT&CK® enterprise tactics of Initial Access, Persistence, Privilege Escalation, Credential Access, Lateral Movement, Exfiltration and Impact.



AS PREDICTED, CLOUD ENVIRONMENT INTRUSIONS INCREASED BY 75% FROM 2022 TO 2023 (FIGURE 2), WITH CLOUD-CONSCIOUS CASES INCREASING BY 110% AND CLOUD-AGNOSTIC CASES INCREASING BY 60%.



Initial Access

Adversaries relied on valid credentials to achieve initial access. They obtained these credentials via accidental credential leakage, brute-force attacks, phishing/social engineering, credential stealers, access brokers, insecure self-service password-reset services and insider threats.

IN THE WILD

FANCY BEAR AND SCATTERED SPIDER COMMONLY TARGETED MICROSOFT 365 CREDENTIALS VIA CREDENTIAL-PHISHING ATTACKS.

Persistence

To maintain access to Azure and Microsoft 365, adversaries commonly achieved persistence at the identity level.

IN THE WILD

ACHIEVING PERSISTENCE AT THE IDENTITY LEVEL IS COMMONLY ACHIEVED BY REGISTERING ADDITIONAL AUTHENTICATION FACTORS IN ENTRA ID.

SCATTERED SPIDER USED AN IDENTITY PROVIDER TO ESTABLISH PERSISTENCE WITH A FEDERATED DOMAIN IN ENTRA ID, INITIALLY RELYING ON AADINTERNALS AZURE AD BACKDOOR.[2] THIS PROVIDED THE ADVERSARY WITH PERSISTENT ACCESS TO MULTIPLE ENTRA ID IDENTITIES. LATER, SCATTERED SPIDER TRANSFERRED THE CONCEPT TO OKTA AND ADDED A FEDERATED IDENTITY PROVIDER TO A VICTIM'S OKTA TENANT.

Privilege Escalation

Adversaries escalated privileges by obtaining access to additional identities from stored credentials, social engineering campaigns or insecure password-reset portals. They also escalated privileges by modifying policies or adding identities to privileged groups or roles.

IN THE WILD

DURING AN INTRUSION TARGETING A NORTH AMERICAN SOFTWARE COMPANY, SCATTERED SPIDER ESCALATED PRIVILEGES BY ATTACHING A NEW ADMINISTRATOR ACCESS POLICY TO A PREEXISTING CLOUD USER, TO WHICH THEY ADDED A NEW ACCESS KEY.

2 https://aadinternals.com/post/aadbackdoor/





Credential Access

Threat actors harvested credentials from password stores and information repositories.

IN THE WILD

INDRIK SPIDER ACCESSED CREDENTIALS STORED IN AZURE KEY VAULT. IN A SEPARATE ATTACK, SCATTERED SPIDER ACCESSED CREDENTIALS STORED IN A CLOUD SECRETS MANAGER, AN IDENTITY-BASED SECRETS AND ENCRYPTION MANAGEMENT SYSTEM, AND SHAREPOINT.

IN ANOTHER CASE, SCATTERED SPIDER ALSO LOCATED A DOMAIN CONTROLLER INSIDE A VICTIM'S AZURE TENANT, COPIED THE DISKS AND CREATED A NEW ADVERSARY-CONTROLLED VIRTUAL MACHINE (VM) INTO WHICH THEY MOUNTED DOMAIN-CONTROLLER DISK COPIES. FROM THOSE DISK COPIES, THE ADVERSARY DUMPED ACTIVE DIRECTORY (AD) DATABASE *NTDS.DIT*.

Lateral Movement

Threat actors moved back and forth between on-premises and cloud environments.

IN THE WILD

SCATTERED SPIDER OFTEN USED ACCESS TO VICTIMS' MICROSOFT 365 ENVIRONMENTS TO SEARCH SHAREPOINT ONLINE FOR VIRTUAL PRIVATE NETWORK (VPN) SETUP INSTRUCTIONS AND THEN LOGGED ON TO THE VPN AND MOVED LATERALLY TO ON-PREMISES SERVERS.

SCATTERED SPIDER WAS ALSO OBSERVED USING AZURE RUN COMMANDS AND SIMILAR CAPABILITIES TO MOVE LATERALLY FROM THE CLOUD CONTROL PLANE TO COMPUTE INSTANCES.

Exfiltration

Adversaries exfiltrated data by using tooling, by directly downloading data from internet-accessible repositories — such as SharePoint Online or GitHub — or by **uploading data to internet-accessible web services.**

IN THE WILD

SCATTERED SPIDER LEVERAGED THE OPEN-SOURCE S3 BROWSER TO EXFILTRATE DATA TO AN EXTERNAL, ADVERSARY-CONTROLLED CLOUD STORAGE BUCKET.

Impact

Some cloud-conscious BGH threat actors targeted cloud storage as part of their operations.

IN THE WILD

CROWDSTRIKE CAO SPECIFICALLY OBSERVED SCATTERED SPIDER ADOPTING BGH TACTICS AND DEPLOYING RANSOMWARE FOR IMPACT.

IN A SEPARATE INCIDENT, AN ALPHA SPIDER AFFILIATE DEPLOYED TOOLING THAT ENABLES *Alphv* TO ENCRYPT AZURE STORAGE FILE SHARES. IN A *LockBit* INCIDENT, INDRIK SPIDER DELETED BACKUPS STORED IN AZURE BACKUPS.

THIRD-PARTY RELATIONSHIP EXPLOITATION

Throughout 2023, targeted intrusion actors consistently attempted to exploit trusted relationships to gain initial access to organizations across multiple verticals and regions. This type of attack takes advantage of vendor-client relationships to deploy malicious tooling via two key techniques: 1) compromising the software supply chain using trusted software to spread malicious tooling and 2) leveraging access to vendors supplying IT services.

Threat actors targeting third-party relationships are motivated by the potential return on investment (ROI): One compromised organization can lead to hundreds or thousands of follow-on targets. These stealthy attacks can also more effectively provide an opportunity for attackers seeking to exploit a hardened end target.



Threat Highlight: Trusted-Relationship Compromises by China-Nexus Adversaries

In 2023, China-nexus adversaries increasingly targeted third-party relationships in efforts to deploy malicious implants and gain initial access. Two adversaries — JACKPOT PANDA and CASCADE PANDA — consistently exploited trusted relationships through supply chain compromises and actor-on-the-side or actor-in-the-middle attacks. In each case, the operations focused on Chinese-speaking victims, possibly indicating ongoing domestic surveillance.

Throughout 2023, JACKPOT PANDA continued to use trojanized executables to deploy malicious utilities or second-stage implants. Beginning in May 2023, the adversary used a trojanized installer for CloudChat, a China-based chat application popular with illegal, Chinese-speaking gambling communities in Mainland China. The trojanized installer served from CloudChat's website contained the first stage of a multi-step process that ultimately deployed *XShade* — a novel implant with code that overlaps with JACKPOT PANDA's unique *CplRAT* implant.

Additional JACKPOT PANDA activity was identified in May 2023 using a signed .NET downloader, dubbed *QuestDownloader*, launched by a LiveHelp100 process. LiveHelp100 is associated with Comm100, a software utility targeted by a JACKPOT PANDA supply chain compromise in September 2022. *QuestDownloader* was ultimately used to deploy *Cobalt Strike* and *UltraVNC*.

Beginning in late 2023, CASCADE PANDA routinely used likely actor-in-the-middle or actor-on-the-side attacks to intercept legitimate update traffic from common utilities, as well as Chinese-language tools, to deploy *WinDealer* — a malicious remote access tool (RAT) uniquely associated with this adversary. In all CASCADE PANDA instances from this time period, legitimate software update processes connected to legitimate infrastructure associated with respective products and legitimate Chinese internet service provider infrastructure.

CASCADE PANDA likely distributes *WinDealer* by using domestic infrastructure to redirect legitimate traffic in transit. In one instance, CASCADE PANDA used a legitimate trojanized Chinese-language translation tool executable to deploy *WinDealer*.

FOR MORE INFORMATION ON ANY OF THE ADVERSARIES MENTIONED IN THIS REPORT AND THOSE TARGETING YOUR INDUSTRY OR REGION, CHECK OUT THE CROWDSTRIKE ADVERSARY UNIVERSE.



Unattributed targeted intrusion actors using TTPs consistent with China-nexus adversaries also exploited trusted relationships to conduct operations in 2023. Throughout the second half of the year, an unattributed actor compromised an India-based information security software vendor and used the resulting access to distribute trojanized executables via legitimate software update processes.

These attacks target victims from multiple regions and industries, including the construction, financial services, government, technology, telecom and logistics sectors throughout the U.S., India, Brazil, Sri Lanka, the Philippines, Zambia, Mexico and Malaysia. Though this trusted-relationship exploitation activity remains unattributed, the final payload used in this attack shares significant code overlaps with *BackShell* and *StealthPipes*, two tools uniquely attributed to WET PANDA.

A second unattributed actor was observed in late 2023 distributing *ShadowPad* to suspected Chinese-speaking targets as part of a likely supply chain compromise. The actor compromised a China-based virtual conference platform and leveraged the resulting access to deploy a trojanized *ShadowPad* installer masquerading as a legitimate software tool. Though this activity is unattributed, *ShadowPad* is exclusively used by China-nexus adversaries such as AQUATIC PANDA, WICKED PANDA and VAPOR PANDA.

In early 2023, an unattributed actor likely compromised an update server associated with iPhone i4Tools management software to deploy *AvanteGarde*, a malware framework associated with China-nexus activity cluster InnateSpark. Though CrowdStrike CAO was able to confirm at least 250 customers had connected to the compromised update server, only 10% received the malicious update, possibly indicating the actor down-selected high-value targets.

Threat Highlight: North Korea's Supply Chain Compromises

Democratic People's Republic of Korea (DPRK) adversaries also demonstrated an increased interest in exploiting trusted relationships in 2023. In particular, LABYRINTH CHOLLIMA abused a trusted relationship between a technology vendor and a client in three instances last year, highlighting an interest in using supply chain compromises as an intrusion vector.

This exploitation tradecraft was first observed in March 2023, when an adversary compromised software at VoIP provider 3CX. This compromise appears to have started with an upstream supply chain compromise of financial technology firm Trading Technologies. The adversary used trojanized 3CX Electron Windows and macOS desktop application variants to deliver information stealers to victim environments. The threat actors then persisted with a July 2023 campaign that similarly abused access to a technology company in efforts to compromise its product and use legitimate infrastructure to infiltrate the compromised company's clientele.



CrowdStrike CAO also observed LABYRINTH CHOLLIMA distributing malware via a trojanized CyberLink media player variant. This campaign stands out among other LABYRINTH CHOLLIMA supply chain compromises, as the adversary used execution guardrails that limited the campaign to a specific geography and temporal window, suggesting the targeting of a particular victim set.

The motivation driving these compromises remains undefined. In one supply chain compromise, CrowdStrike CAO detected trojanized software in the environments of 62 customers; however, subsequent supply chain compromises were more limited in scope. The adversary may be using supply chain compromises to cast a wide net and deliver appropriate follow-on tooling to interesting targets.

LABYRINTH CHOLLIMA is equally likely abusing trusted relationships between suppliers and product users to infiltrate specific high-value targets for currency generation and espionage campaigns. CrowdStrike CAO assesses that additional LABYRINTH CHOLLIMA supply chain compromises are increasingly likely to occur in the near future. The adversary likely considers supply chain compromise a useful tactic with potential to streamline operations. This assessment is made with moderate confidence based on the volume of supply chain compromises observed in 2023.

Outlook:
Third-Party Relationship Exploitation

Trusted-relationship compromises will continue to attract targeted intrusion actors in the immediate future. The high ROI for these attacks, particularly in terms of access to potential downstream compromises relative to the limited effort required to compromise one target, will likely motivate attacks throughout 2024.

Organizations operating in the technology sector are uniquely at risk from third-party relationship exploitation. In 2023, nearly every trusted-relationship compromise originated as part of an intrusion at a technology sector organization that provided commercial software.

VULNERABILITY LANDSCAPE: "UNDER THE RADAR" EXPLOITATION

Threat actors have adapted to the enhanced visibility of traditional endpoint detection and response (EDR) sensors by altering their exploitation tactics for initial access and lateral movement. They are now targeting the network periphery, where defender visibility is reduced by the possibility that endpoints may lack EDR sensors or cannot support sensor deployment (Figure 3).

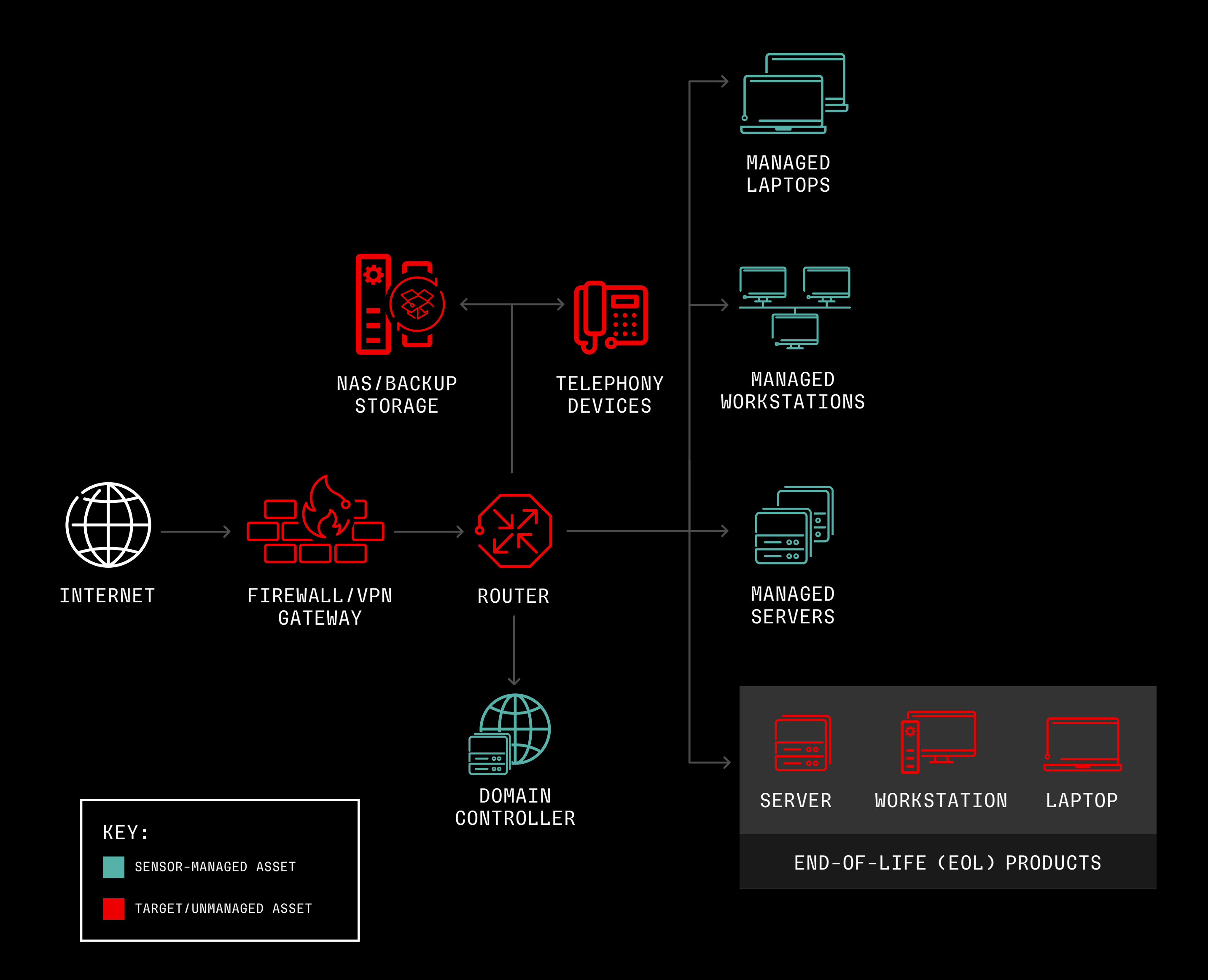


Figure 3. Unmanaged targets on a generic network

Unmanaged network appliances — particularly edge gateway devices — remained the most routinely observed initial access vector for exploitation during 2023. These devices are commonly based on obsolete architecture, leading to broadly exploited vulnerabilities in firewall and VPN platforms from Cisco (CVE-2023-20198), Citrix (CVE-2023-3519, CVE-2023-4966) and F5 (CVE-2023-46747).



UNMANAGED NETWORK APPLIANCES — PARTICULARLY EDGE GATEWAY DEVICES — REMAINED THE MOST ROUTINELY OBSERVED INITIAL ACCESS VECTOR FOR EXPLOITATION DURING 2023.

Exploitation was also observed in various other unmanaged devices throughout 2023. Targeted intrusion actors likely engaged in opportunistic Ivanti mobile device management application targeting via CVE-2023-35078 and CVE-2023-35082. *Akira* ransomware operators leveraged exploits for CVE-2023-27532 — a vulnerability in Veeam Backup & Replication — to pivot into victim backup storage infrastructure. Additionally, eCrime actors developed zero-day exploits for telephony products based on an abandoned open-source project.

The latter zero-day exploit relates to another trend observed in 2023: a focus on EOL product exploitation. Threat actors are actively developing exploits for EOL products that cannot be patched and often do not allow for modern sensor deployment. Unsupported operating system (OS) servers and legacy gateway appliances offer easy access — even to otherwise antiquated malware families — leading to lingering infections that distract resources from contemporary security issues.



THREAT ACTORS ARE ACTIVELY DEVELOPING EXPLOITS FOR EOL PRODUCTS THAT CANNOT BE PATCHED AND OFTEN DO NOT ALLOW FOR MODERN SENSOR DEPLOYMENT.

Increasing defender visibility to such exploit vectors is key in mitigating the risk posed by these tactics. CrowdStrike® Falcon Surface℠ can be leveraged to monitor and reduce internet-exposed services and maintain an application inventory across an organization's attack surface. Defenders should prioritize patching exposed products, particularly open-source platforms, when the products are subject to known remote code execution (RCE) vulnerabilities. Finally, CrowdStrike Falcon® Spotlight can determine whether sensor-deployed assets are subject to known vulnerabilities and when these endpoints have reached EOL.

2023 ISRAEL-HAMAS CONFLICT: CYBER OPERATIONS FOCUS ON DISRUPTION AND INFLUENCE

On October 7, 2023, Hamas military wing Izz al-Din al-Qassam Brigades (IDQB) and several other Gaza-based militant groups launched a massive kinetic attack against Israel, killing hundreds of Israelis and taking hostages. In the ensuing months, CrowdStrike CAO tracked ongoing cyber operations from targeted intrusion and hacktivist actors. Activity and claims from both groups primarily focus on targeting operational technology or other critical systems — likely to psychologically influence target populations — and deploying destructive wipers against Israeli or Israel-linked entities.

Most conflict-driven cyber operations observed include hacktivist activity and operations by suspected faketivists. Within the context of the Israel-Hamas conflict, the dividing line between these two threat actor types has blurred, as genuine hacktivist groups often amplify the claims of, or provide support to, likely state-nexus inauthentic personas.

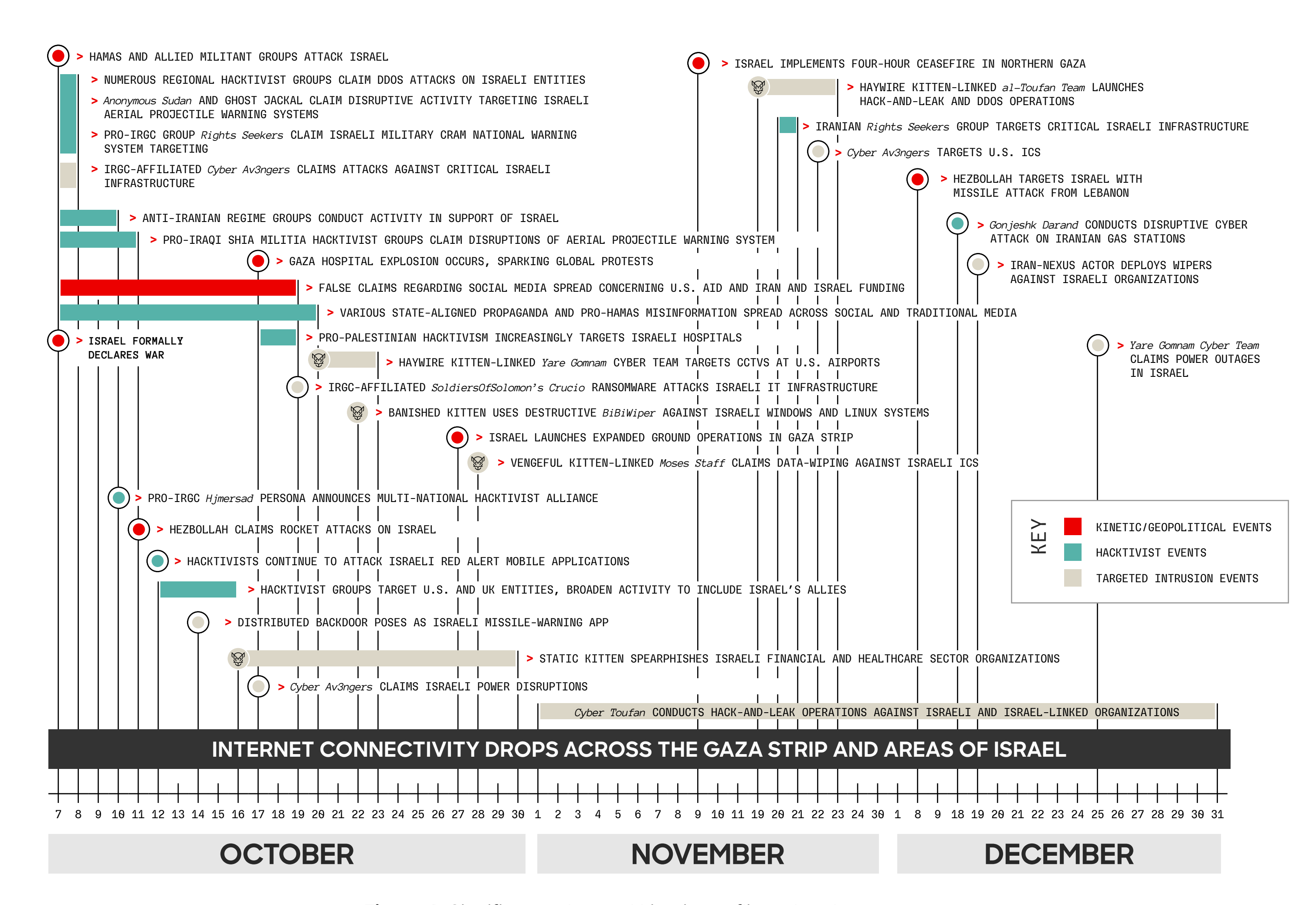


Figure 4. Significant cyber and kinetic conflict-related events

Faketivists associated with Iranian state-nexus adversaries and hacktivists branding themselves as "pro-Palestinian" focused on targeting critical infrastructure, Israeli aerial projectile warning systems and activity intended for information operation purposes in 2023.

Though CrowdStrike CAO tracks multiple adversaries associated with the Hamas militant group, activity attributed to these adversaries has not been observed in connection with the Israel-Hamas conflict to date. This is likely due to unavailable resources or the degradation of internet and electricity-distribution infrastructure in the conflict zone.

Faketivism

INTRODUCED IN THE CROWDSTRIKE 2016 GLOBAL THREAT REPORT, FAKETIVISM REFERS TO ACTIVITY BY ENTITIES THAT CHARACTERIZE THEMSELVES AS HACKTIVIST GROUPS BUT MORE LIKELY REPRESENT A FRONT FOR A GOVERNMENT OR OTHERWISE PROFESSIONAL ENTITY.

IN AN EFFORT TO APPEAR GENUINE, FAKETIVISTS — AKA INAUTHENTIC PERSONAS — OFTEN ADOPT THE EXISTING IMAGERY, RHETORIC, TTPS AND SOMETIMES NAMES OF ESTABLISHED HACKTIVISTS. THEY OFTEN SURFACE IN DIRECT RESPONSE TO GEOPOLITICAL EVENTS, OFTEN HAVE LITTLE OR NO ESTABLISHED ACTIVITY HISTORY, AND ALMOST ALWAYS OPERATE IN DIRECT ALIGNMENT WITH STATE GOVERNMENT INTERESTS. THESE PERSONAS PROVIDE STATE BACKERS WITH A LAYER OF DENIABILITY BUT CAN ALSO SERVE INFORMATION OPERATIONS GOALS.

Hamas-Nexus Adversaries Noticeably Absent from Conflict-Related Activity

CrowdStrike CAO-assessed, likely Gaza-based adversaries EXTREME JACKAL and RENEGADE JACKAL demonstrate support for strategic Hamas interests. Additionally, evidence suggests the CruelAlchemy activity cluster represents a Hamas-linked cyber operations unit physically present in Turkey.

RENEGADE JACKAL was the most active Hamas-nexus adversary throughout 2023. The group primarily targeted Middle East-based government entities with its custom *Micropsia* Windows malware and Android implants. In mid-October 2023, CrowdStrike CAO linked RENEGADE JACKAL to the *Jerusalem Electronic Army*, an ostensible hacktivist group Hamas officials previously indicated was in support of the IDQB Cyberwarfare Unit.

Open-source reporting identified activity, allegedly attributable to Hamas, targeting Israeli Defense Forces (IDF) personnel. However, CrowdStrike CAO has no further evidence to suggest the aforementioned adversaries are currently targeting Israeli entities in connection with recent events in Israel and Gaza.[3] Since the onset of the conflict, internet connectivity in the Gaza Strip has been significantly degraded almost certainly due to a combination of kinetic activity, power outages and distributed denial-of-service (DDoS) attacks.

Power and internet disruptions have likely hindered Gaza-based adversary operations. Though no CruelAlchemy activity has been observed in direct association with the Israel-Hamas conflict, identified command-and-control (C2) infrastructure indicates the actor remained active following the onset of the conflict, possibly supporting prior reporting that suggests CruelAlchemy operates from outside of Gaza.

Widespread Hacktivist Operations Span Motivational Spectrum, Demonstrate Concerted Interest in Critical Systems

Though the October 7, 2023, launch of the Israel-Hamas conflict ignited a flurry of pro-Palestine and pro-Israel hacktivist activity, the former far outpaced the latter. Known and previously unobserved hacktivists within the conflict region and from around the world claimed the activity, a significant portion of which revolved around attempted or alleged aerial projectile warning system and critical infrastructure disruption targeting Israel. A smaller number of hacktivists also extended their operations beyond the conflict region to target countries or entities deemed supportive of Israel.

3 https://www.timesofisrael.com/liveblog_entry/idf-exposes-catfishing-network-seeking-to-extract-info-from-troops-on-hamass-behalf/



Aerial Projectile Warning Systems and Critical Infrastructure Targeting

Multiple hacktivist entities have targeted aerial projectile warning systems in Israel and claimed to have disrupted IDF counter-rocket, artillery and mortar systems to prevent notification delivery and/or send false imminent attack notifications to Israeli citizens. Observed targeting of these services decreased after mid-October 2023; however, a surge of kinetic activity in the region could ignite a renewed interest in further disruption or false notifications.

Throughout the duration of the conflict, pro-Palestine hacktivists have consistently targeted critical infrastructure in Israel, including disruptive activity against energy-distribution infrastructure and water pumps, DDoS attacks against utility companies, and hack-and-leak operations against water treatment and energy plants. This activity is likely an attempt to inflict physical and psychological damage on Israeli citizens and will likely continue throughout the duration of the Israel-Hamas conflict. This assessment is made with high confidence based on consistent targeting to date and similar activity observed in other recent conflicts, such as the Russia-Ukraine war.

Operations Beyond the Immediate Conflict Region

Limited hacktivist activity extended beyond the immediate conflict area in retaliation against real or perceived support of Israel. On October 12, 2023, Yemeni group *Team R70* claimed a DDoS attack against a U.S.-based airport, alleging the airport receives the most Israeli air traffic.

On October 14, 2023, prominent South Asian hacktivist group *Team Insane Pakistan* claimed a DDoS attack against a British military website. This activity was accompanied by references to U.K. support for Israel.

On October 16, 2023, a likely Indonesian hacktivist group calling itself *INFINITE INSIGHT* shared leaked data, claiming to have breached the personally identifiable information (PII) of nearly 790,000 doctors in the United States. The alleged leak was reportedly in retaliation against U.S. support for Israel as well as to show support for Palestinians.

Hacktivists will likely continue limited targeting of countries and entities beyond the conflict region that they perceive as supporting Israel. This assessment is made with high confidence based on consistent activity observed to date and in similar conflicts, such as the Russia-Ukraine war, as well as observed communications within hacktivist channels.



Iranian Adversaries Operate Inauthentic Personas for Disruption and IO

CrowdStrike CAO has not observed Iranian state-nexus adversaries providing direct operational support to Hamas' cyber units or IDQB's kinetic operations. Iranian adversaries associated with the country's Ministry of Intelligence and Security (MOIS) and Islamic Revolutionary Guard Corps (IRGC) have an established record of using disruptive and destructive attacks, hack-and-leak operations, inauthentic personas and hacktivist groups to target Israeli entities.

This cyber-enabled activity is likely intended to influence Israeli audiences during the ongoing crisis. Though Iranian cyber operations have historically focused on Israel, the number of faketivist personas leveraged against Israeli targets has increased since the onset of the Israel-Hamas conflict. These personas' claims focus on campaign impacts on operational technology and are almost certainly intended to influence the target populations' perception of Iranian adversaries' ability to disrupt critical services.



Figure 5. Iran-nexus cyber activity during the conflict

Adversary	Date in 2023	Activity
SPECTRAL KITTEN	OCTOBER 9	*MALEKTEAM* PERSONA LEAKED PII, CCTV FOOTAGE AND OTHER DATA ALLEGEDLY SOURCED FROM INTRUSIONS TARGETING ISRAELI ENTITIES
HAYWIRE KITTEN	OCTOBER-NOVEMBER	HAYWIRE KITTEN, ASSOCIATED WITH IRGC CONTRACTOR EMENNET PASARGAD, OPERATED PERSONAS *YARE GOMNAM CYBER TEAM* AND *AL-TOUFAN TEAM* TO CLAIM CCTV SYSTEM TARGETING AT U.S. AIRPORTS, THREATEN CYBER-ENABLED KINETIC ATTACKS AGAINST ISRAEL, AND CARRY OUT HACK-AND-LEAK AND DDOS OPERATIONS
BANISHED KITTEN	OCTOBER	MOIS-LINKED BANISHED KITTEN DEPLOYED THE *BIBIWIPER* MALWARE FAMILY AGAINST COMPANIES IN ISRAEL; A *KARMA POWER* ANTI-ISRAELI MESSAGING CAMPAIGN OCCURRED ALONGSIDE THE REPORTED WIPER OPERATIONS
VENGEFUL KITTEN	OCTOBER 26-28	*MOSES STAFF* CLAIMED DATA-WIPING ACTIVITY AGAINST MORE THAN 20 COMPANIES' INDUSTRIAL CONTROL SYSTEMS (ICS) IN ISRAEL AND INDICATED INTEREST IN SMS, BASE-TRANSCEIVER STATIONS AND PUBLIC ALERT SYSTEMS
UNATTRIBUTED IRGC-NEXUS PERSONAS	OCTOBER-NOVEMBER	IRGC-LINKED *SOLDIERSOFSOLOMON* USED DESTRUCTIVE RANSOMWARE VARIANT *CRUCIO* AGAINST INTERNET OF THINGS (IoT) DEVICES IN ISRAEL; IRGC-AFFILIATED *CYBER AV3NGERS* COMPROMISED AND DEFACED PROGRAMMABLE LOGIC CONTROLLERS (PLCs) IN ISRAEL AND THE U.S. AT CRITICAL INFRASTRUCTURE ENTITIES SUCH AS WATER TREATMENT FACILITIES[4]
UNKNOWN IRAN-NEXUS ACTOR	DECEMBER 19	UNKNOWN IRAN-NEXUS ACTOR DEPLOYED WIPERS AGAINST ISRAELI ORGANIZATIONS
HAYWIRE KITTEN	DECEMBER 25	*YARE GOMNAM CYBER TEAM* CLAIMED RESPONSIBILITY FOR POWER OUTAGES IN ISRAEL

4 https://www.cisa.gov/news-events/alerts/2023/12/01/cisa-and-partners-release-joint-advisory-irgc-affiliated-cyber-actors-exploiting-plcs



Outlook:
Cyber Operations in the Conflict

Unlike in the Russia-Ukraine war, where known cyber operations have directly contributed to the conflict, those involved in the Israel-Hamas conflict have not directly contributed to Hamas' military operations against Israel. The full breadth and effects of activity targeting Israel, particularly by Iranian state-nexus adversaries and allied proxies, are almost certainly not fully known. However, identified incidents have largely been misaligned with early concerns that Iranian cyberattacks could cause significant disruptions across critical sectors in Israel and broaden in scope to allied countries. This misalignment may point to Iranian forces' incapability or lack of preparedness and their desire to avoid an unintended escalation that could draw Iran more directly into the conflict.

CrowdStrike CAO tracks activity clusters SpoiledMocha and Moonshuttle. These are reportedly aligned with Iran's regional proxies — the Houthi movement in Yemen and Hezbollah in Lebanon, respectively — even though these entities have not yet been observed within the Israel-Hamas conflict context.

Pro-Iraqi Shia militia hacktivist groups have demonstrated consistent involvement in targeting Israeli entities since the onset of the conflict. An escalation in kinetic hostilities could lead to related activity from these groups.

Hacktivist activity will almost certainly continue apace with fluctuations in related geopolitical developments. This assessment is made with high confidence based on the activity patterns exhibited to date as well as consistent patterns observed across other similar conflicts.



THREATS ON THE 2024 HORIZON

As organizations plan for potential threats emerging in 2024, two potential disruption drivers come to the forefront: generative AI and 2024 global government elections.

Generative AI Use Within the Threat Landscape

Mainstream accessible generative AI technology exploded in late 2022, opening up a new realm of possibilities for efficient content creation and drawing the attention of adversaries seeking ways to exploit this new technology for their own purposes.

Generative AI has massively democratized computing to improve adversary operations. It can also potentially lower the entry barrier to the threat landscape for less sophisticated threat actors.

Two primary generative AI opportunity areas within the threat landscape include:

- Developing and/or executing malicious computer network operations (CNO), including tool and resource development such as scripts or code that could be functionally malicious if used correctly
- Supporting the efficiency and effectiveness of social engineering and information operations campaigns



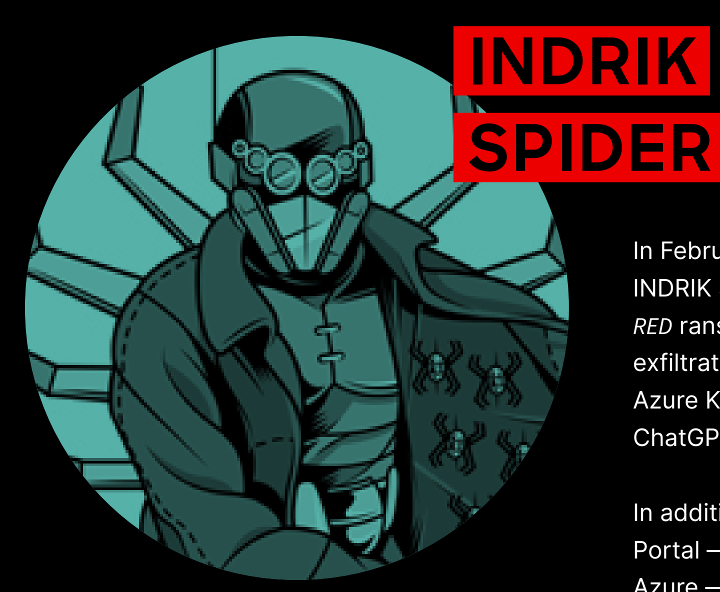
GENERATIVE AI HAS MASSIVELY DEMOCRATIZED COMPUTING TO IMPROVE ADVERSARY OPERATIONS. IT CAN ALSO POTENTIALLY LOWER THE ENTRY BARRIER TO THE THREAT LANDSCAPE FOR LESS SOPHISTICATED THREAT ACTORS.

Generative AI in Malicious Computer Network Operations

It's difficult to confidently gauge the probability of adversaries using newer technologies such as generative AI in their operations, particularly in relation to how these technologies will support malicious CNO. Only rare concrete observations included likely adversary use of generative AI during some operational phases.

CrowdStrike's visibility into the use of such tools is likely incomplete. This is either a result of limited observations, the fact that the AI-generated material did not intrinsically leave significant indicators of its true nature or adversaries taking steps to avoid revealing evidence that generative AI was in use.

Throughout 2023, generative AI was rarely observed supporting malicious CNO development and/or execution.



INDRIK SPIDER

In February 2023, CrowdStrike Services responded to an INDRIK SPIDER incident involving BITWISE SPIDER's *LockBit RED* ransomware. During this incident, INDRIK SPIDER exfiltrated credentials from cloud-based credential manager Azure Key Vault. Logs show that INDRIK SPIDER also visited ChatGPT while interacting with the Azure Portal.

In addition to visiting ChatGPT while browsing the Azure Portal — presumably to understand how to navigate in Azure — browsing activity analysis indicates INDRIK SPIDER used search engines such as Google and Bing and searched on GitHub during the operations to understand how to exfiltrate Azure Key Vault credentials.

Using search engines and visiting ChatGPT indicate that though INDRIK SPIDER is likely new to the cloud and not yet sophisticated in this domain, it is using generative AI to fill these knowledge gaps.



SCATTERED SPIDER

In the second half of 2023, SCATTERED SPIDER used the Azure AD PowerShell module to download all Entra ID user immutable IDs at a North American financial services victim. Using its Entra ID backdoor, the adversary could log in as any of the downloaded users. The PowerShell used to download the users' immutable IDs resembled large language model (LLM) outputs such as those from ChatGPT. In particular, the pattern of one comment, the actual command and then a new line for each command matches the Llama 2 70B model output.

Based on the similar code style, SCATTERED SPIDER likely relied on an LLM to generate the PowerShell script in this activity.



Generative AI in Social Engineering and Information Operations

In recent years, certain language models have been able to compose fictional stories[5] and generate digital artwork.[6] Since at least mid-2021, CrowdStrike has frequently reported on alleged research interest in highly deceptive AI-fabricated images, audio and video (aka "deepfakes") by Russia, China and Iran. Researchers and academics have further speculated that threat actors will almost certainly use generative AI tools in information and influence operations in the near future.[7]

These speculations began actualizing in 2023: A Chinese information operations campaign, likely reliant on images produced by generative AI (specifically diffusion-model-generated images), gained authentic engagement across several prominent social media platforms throughout September. Beyond state-nexus actors, CrowdStrike also observed a hacktivist group attempting to create a spam tool using generative AI as part of its efforts to disseminate pro-Azerbaijan messaging.

Outlook

Generative AI has potential for use in numerous fields not likely identified or popularized in mainstream public discourse. AI's continuous development will undoubtedly increase the potency of its potential misuse — particularly within the scope of information operations and especially for less digitally literate audiences. The degree to which popular generative AI tools can be used maliciously will likely adapt over time as companies, tool owners and governments respond to new developments and perceived misuse.

CrowdStrike CAO assesses that generative AI will likely be used for cyber activities in 2024 as the technology continues to gain popularity. The team will track exactly how threat actors use this technology, and how this use differs from mainstream applications, throughout 2024. This type of research includes examinations of both:

- The potential that adversaries will use publicly available or open-source LLMs, which will likely require continual adversary navigation around safeguards against malicious or illegal activity (e.g., jailbreaking).
- Adversaries' attempts to develop their own models or generative AI tools that require less prompt engineering. Notably, the cost of training LLMs can significantly deter their independent, illicit development. Threat actors' attempts to craft and use such models in 2023 frequently amounted to scams that created relatively poor outputs and, in many cases, quickly became defunct.

---

5 https://apnews.com/article/7f49bd9aa9d1427d8400e40beb9f5ba4
6 https://apnews.com/article/artificial-intelligence-images-rights-1c6d9e0e260e2d135a3e3bf98d5493df
7 https://cdn.openai.com/papers/forecasting-misuse.pdf

2024 Elections

In 2024, individuals from 55 countries representing more than 42% of the global population will participate in presidential, parliamentary and/or general elections. This includes seven of the 10 most populous countries in the world: India, the U.S., Indonesia, Pakistan, Bangladesh, Russia and Mexico. High-profile, national-level elections will also occur in countries or groups involved in, or proximal to, major geopolitical conflicts. These include Taiwan, Azerbaijan, India, Pakistan, Iran, Belarus, Russia, Finland, Lithuania and the European Union.

2024's potential to transform geopolitics around the globe for the near future will likely give adversaries numerous opportunities, and a considerable strategic impetus, to target entities involved in electoral processes throughout the coming year.

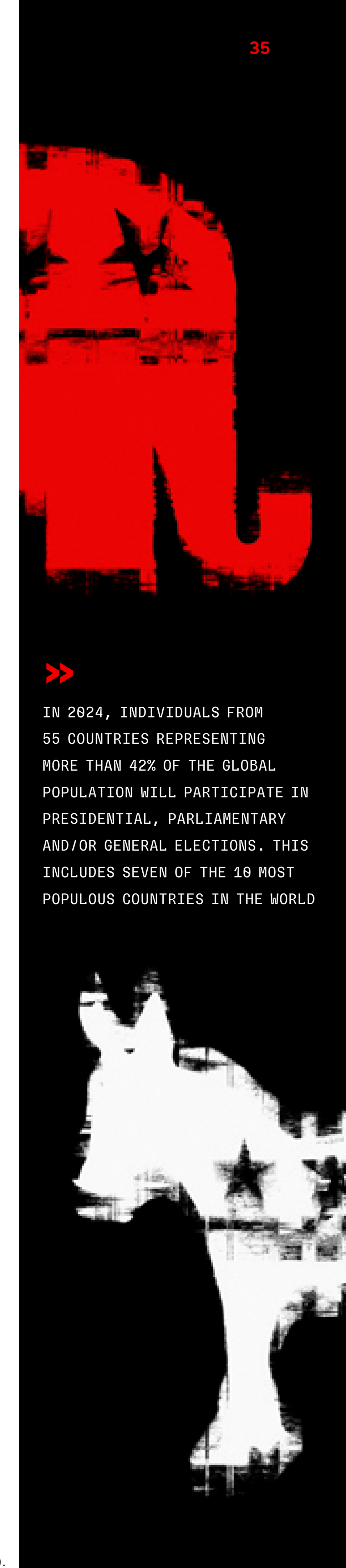
Election Targeting

Cyber activity targeting elections can range from direct attempts to disrupt electoral processes to more indirect efforts to sway voter opinion toward outcomes preferred by the adversary.[8] The most direct, but least frequent, targeting involves intrusions against the software and hardware used to record, tally, count and transmit votes in voting systems. This form of election interference can range from using computer network attacks to intentionally disrupt, degrade or destroy voting systems to using privileged access or vulnerabilities to attempt to alter vote counts without detection.

Less direct forms of targeted intrusion can involve attempts to compromise, disrupt access to or leak data from government systems that provide logistical information to voters, store voter registration data or otherwise support transparent and democratic election conduct. These targeted intrusion efforts include using DDoS attacks or website defacements against local, municipal, provincial and state government systems, a tactic historically favored by hacktivists seeking to espouse their viewpoints during tense political moments. Other parties involved in elections — such as political candidates, parties, donors and advocacy groups — can also be targeted in a variety of ways, including via the use of hack-and-leak operations often designed to publicly discredit the target.

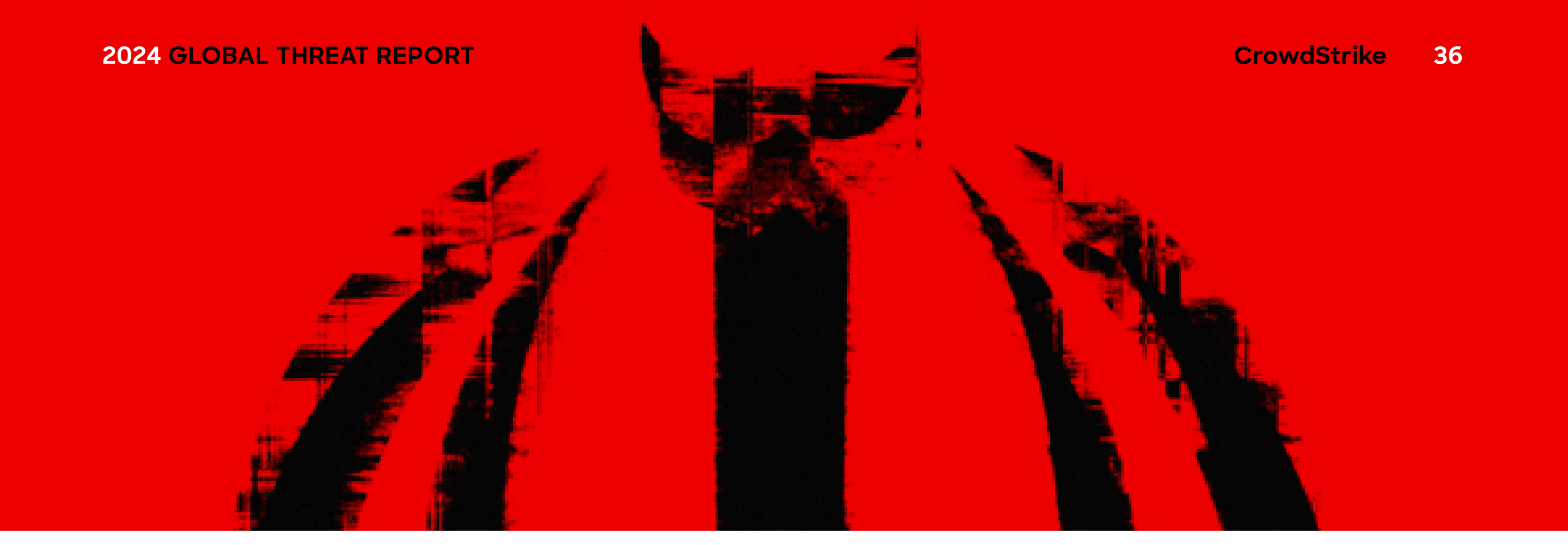
The least direct type of election targeting — but almost certainly the most common and typically the most difficult to prevent — involves distributing mis- or disinformation to electorates before, during and after voting processes in an effort to influence popular opinion.

These information operations can take many forms. One common theme involves attempts to generate disruptive narratives — for example, they may undermine public confidence in election outcomes, enhance perceptions that specific political parties or individuals are corrupt, impugn candidates' personal character or disseminate inflammatory and polarizing social rhetoric. Other operations may aim to reinforce perspectives that portray the threat actor responsible in a more positive light; for example, as an advocate for specific policy positions beneficial to that entity or representative of cooperation or coexistence rhetoric.



IN 2024, INDIVIDUALS FROM 55 COUNTRIES REPRESENTING MORE THAN 42% OF THE GLOBAL POPULATION WILL PARTICIPATE IN PRESIDENTIAL, PARLIAMENTARY AND/OR GENERAL ELECTIONS. THIS INCLUDES SEVEN OF THE 10 MOST POPULOUS COUNTRIES IN THE WORLD

8 Though this section details the actions of external malicious actors targeting elections, it is worth noting that ostensibly democratic governments sometimes also use their own domestic security authorities to legally restrict the free flow of information during election cycles (e.g., internet shutdowns and censorship).



Threat Highlight: Iranian Targeting of U.S. Elections in 2020

In late October 2020, a few weeks before the last U.S. presidential election cycle, Iranian threat actors conducted varied targeted IO against U.S. entities. They sent threatening emails to voters, alleging to represent a far-right U.S. political group and directing recipients to vote for a specific candidate. Iranian threat actors also disseminated a video falsely alleging to depict overseas actors fabricating ballots, implying one particular political party would seek to exploit security vulnerabilities and compromise voting systems.

Outlook

The most common malicious activities targeting elections have historically involved information operations likely conducted by state-nexus entities against citizens of countries that hold specific geopolitical interest to the threat actor and simple, short-lived hacktivism — including DDoS attacks and website defacements — against state and local government entities. This trend is highly likely to continue in 2024.

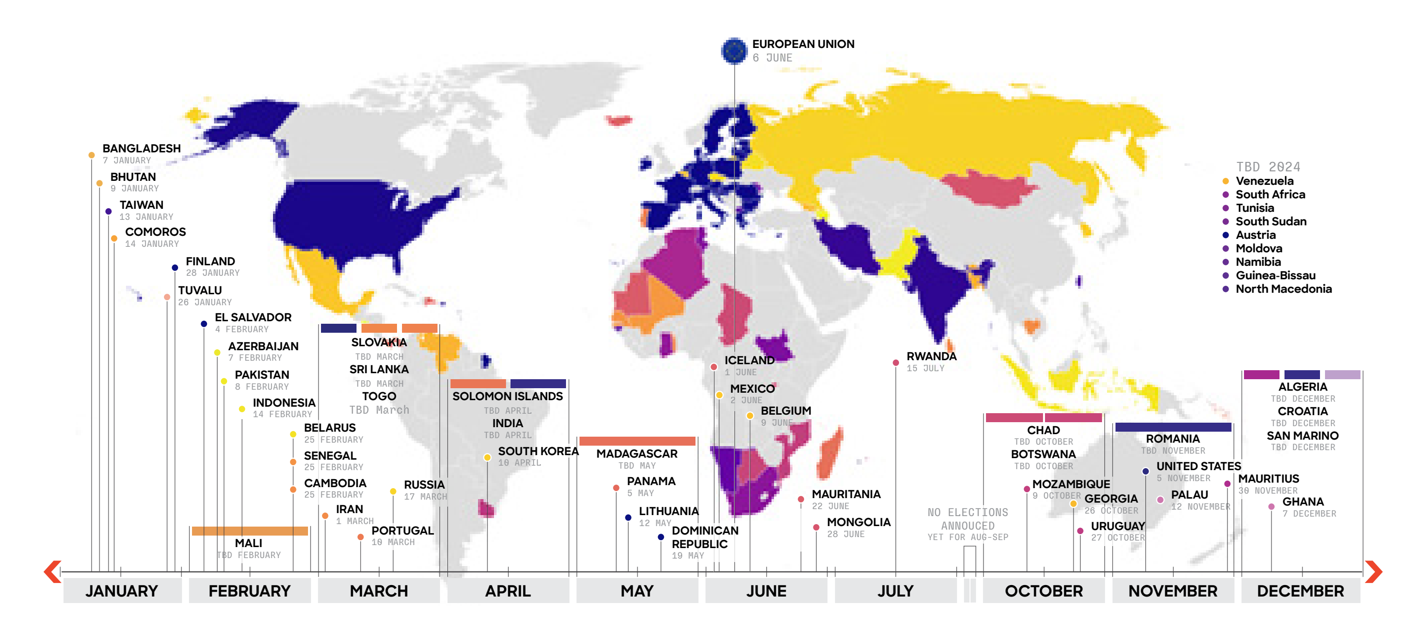


Figure 6. Countries holding presidential, parliamentary or general elections in 2024

In 2024, countries of interest involved in election cycles will likely be at risk of significant and lengthy IO campaigns from major global powers. Russia and Iran will likely leverage IO against the U.S. and the EU, which they consider major geopolitical opponents.

China will also likely conduct IO against elections held in its perceived regional sphere of influence, such as those in Indonesia, South Korea and Taiwan. Russia will almost certainly behave similarly in elections occurring in Belarus, Lithuania, Finland and Georgia. India and Pakistan are highly likely to conduct significant IO campaigns against one another during their respective elections in April and February 2024, particularly given the current political upheaval and polarization in both countries.[9]

Given the ease with which AI tools can generate deceptive but convincing narratives, adversaries will highly likely use such tools to conduct IO against elections in 2024. Politically active partisans within those countries holding elections will also likely use generative AI to create disinformation to disseminate within their own circles.

These issues were already observed within the first few weeks of 2024, as Chinese actors used AI-generated content in social media influence campaigns to disseminate content critical of Taiwan presidential election candidates.

The overall polarization of the political spectrum in many countries amid continuing economic and social issues will likely increase the susceptibility of those countries' citizenries to IO — particularly IO campaigns targeted at reinforcing those individuals' negative opinions of political opponents.[10]

Additionally, changes to or staff reductions affecting the enforceability of content moderation policies at major social media companies will likely provide opportunities for adversary exploitation using these platforms to disseminate IO narratives.[11]

With such political environments currently existing in most of the large and geopolitically significant countries, 2024 will almost certainly present a challenging global test for democracies.

>>

RUSSIA AND IRAN WILL LIKELY LEVERAGE IO AGAINST THE U.S. AND THE EU, WHICH THEY CONSIDER MAJOR GEOPOLITICAL OPPONENTS.

---

9 https://www.eastasiaforum.org/2024/01/06/military-influence-and-political-peril-in-pakistan/
https://foreignpolicy.com/2024/01/02/india-elections-modi-bjp-congress-nda-lok-sabha-brics/

10 https://www.cambridge.org/core/journals/american-political-science-review/article/abs/partisan-polarization-is-the-primary-psychological-motivation-behind-political-fake-news-sharing-on-twitter/3F7D2098CD87AE5501F7AD4A7FA83602

11 https://www.theguardian.com/media/2023/dec/07/2024-elections-social-media-content-safety-policies-moderation

eCrime Landscape

The CrowdStrike eCrime Index® (ECX) tracks activity — including the number of observed spam emails and the average cost of buying access to a corporate network — across multiple eCrime ecosystem segments and calculates the total number of observed ransomware victims.

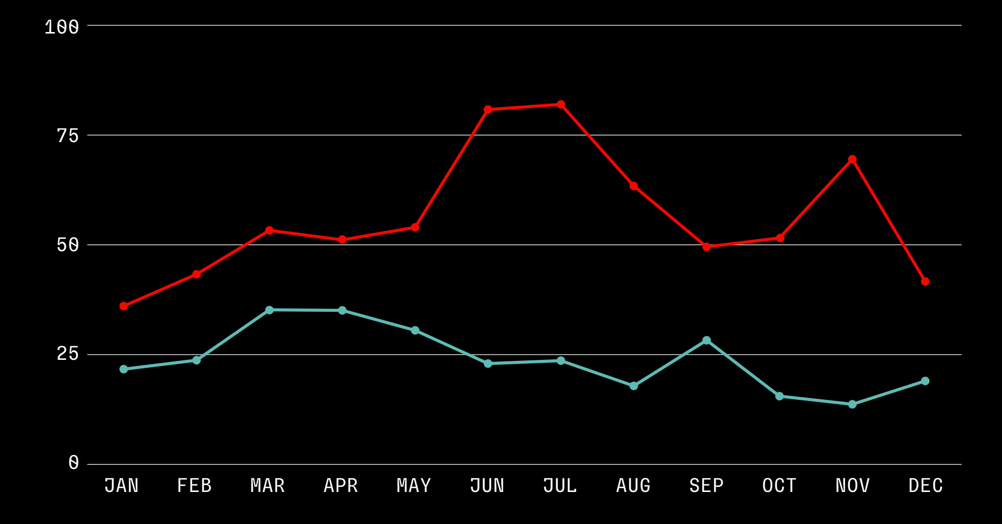
Until May 2023, the ECX exhibited trends similar to those observed in 2022. However, from June 2023 onward, the ECX grew significantly, with major spikes between June and August. The most impactful contributors to these spikes included high BGH incident frequency and a sudden increase in observed DDoS attacks.

The ECX spiked again in November 2023, reflecting increases in spam email numbers and the rising average price for loaders and stealers.

2023

2022

ECX Value= **+67%**



New Vulnerabilities with 9/10 CVSS3 Score
+6%

BGH Incidents Involving Data Leaks
+76%

Average Loader Cost
+169%

Average Crypter Cost
+250%

Average Stealer Cost
+286%

Average Ransom Demand
-27%

Identified Spam Emails
-15%

Figure 7. eCrime index value, 2022 vs. 2023, and key observable changes, 2023

The 2023 ECX tracked the most annual activity to date, representing the index's year-over-year growth. Spam emails likely decreased in 2023 as adversaries searched for other means of initial access and after a multinational operation shut down MALLARD SPIDER's *QakBot*.

Though the average ransom demand was lower in 2023 than in 2022, this highly likely represents an outlier in the dataset and not an accurate view of the threat landscape. Ransom demands have likely remained consistently high throughout this period, but the ability to track these values is becoming challenging due to threat actors and victims implementing stricter privacy measures around ransom price demands and payments.

BIG GAME HUNTING

2023 BGH DLS Statistics

The number of victims named on BGH dedicated leak sites increased significantly in 2023, with 4,615 victim posts made to DLSs — a 76% increase over 2022. Several factors contributed to this growth, including newly emerged BGH adversaries, growth of existing adversary operations and select high-volume campaigns such as multiple GRACEFUL SPIDER zero-day exploitations.



THE NUMBER OF VICTIMS NAMED ON BGH DEDICATED LEAK SITES INCREASED SIGNIFICANTLY IN 2023, WITH 4,615 VICTIM POSTS MADE TO DLSs — A 76% INCREASE OVER 2022.

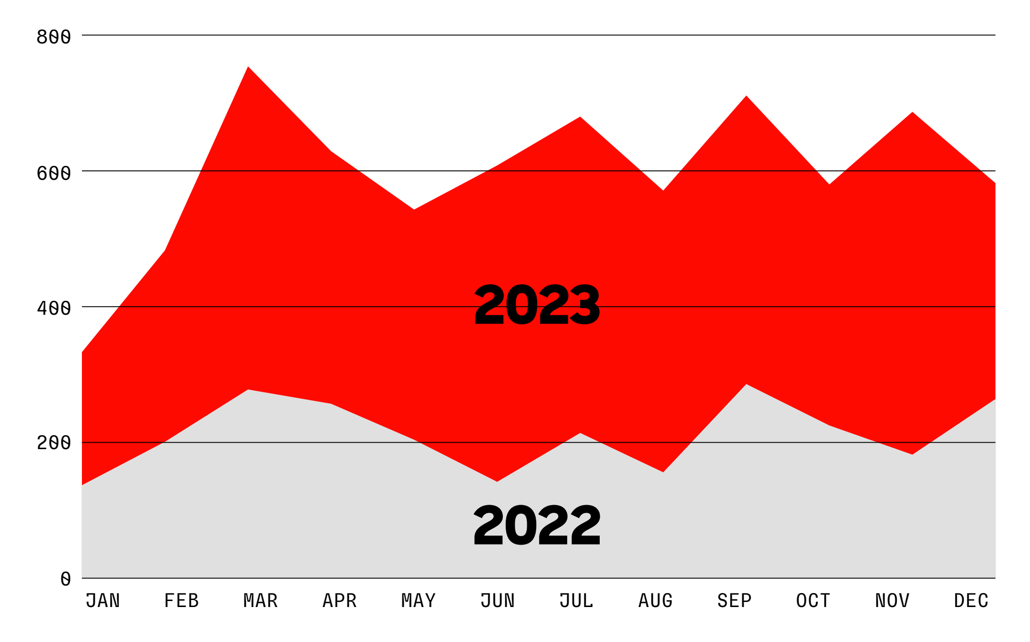


Figure 8. DLS post quantity, 2022 vs. 2023

Collectively, BITWISE SPIDER, ALPHA SPIDER, GRACEFUL SPIDER, RECESS SPIDER and BRAIN SPIDER accounted for 77% of posts across all tracked adversary DLSs. BITWISE SPIDER and ALPHA SPIDER have historically posted numerous new DLS posts and were ranked in first and second place, respectively, for the highest number of DLS posts in 2022 and 2023.

RECESS SPIDER and BRAIN SPIDER started their own ransomware operations in mid-2022 and January 2023, respectively. They have since grown in prominence to account for the fourth (RECESS SPIDER) and fifth-highest (BRAIN SPIDER) number of DLS posts in 2023.

GRACEFUL SPIDER — which has operated since 2016 and has typically conducted low-volume campaigns — exploited three zero-day vulnerabilities in 2023 to exfiltrate data from hundreds of victims across the globe. This adversary ultimately published the third-highest number of DLS posts in 2023.

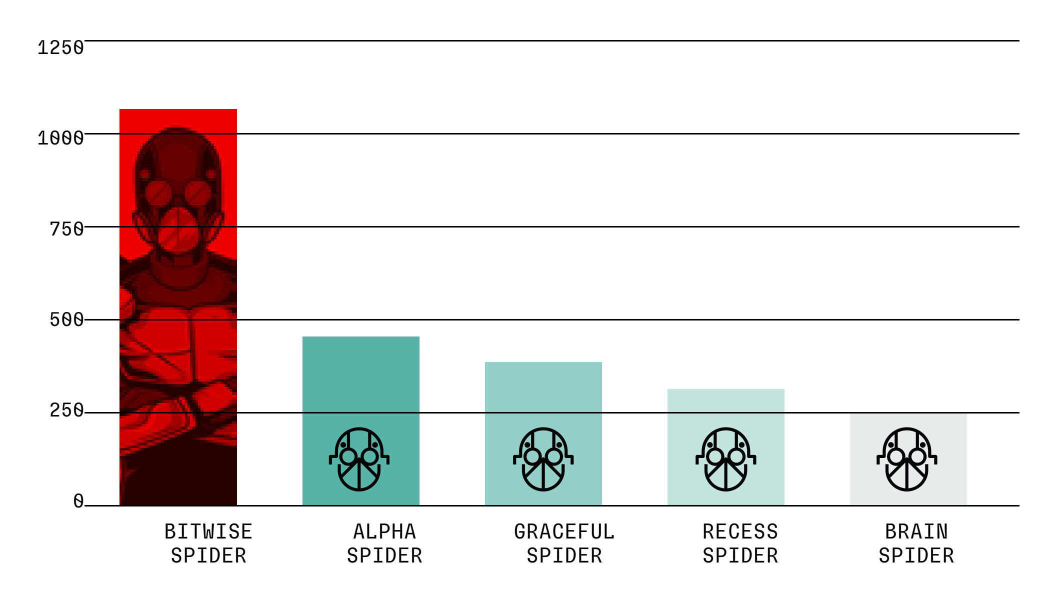


Figure 9. Top five adversaries by DLS posts, 2023

SCATTERED SPIDER Adopts Ransomware as Primary Monetization Method

SCATTERED SPIDER began using ALPHA SPIDER's *Alphv* ransomware in April 2023. The adversary had previously monetized intrusions by selling victim data and SIM swaps as well as stealing cryptocurrency. Adopting ransomware as its primary means of extortion has shifted the scope of the adversary's target profile: Most SCATTERED SPIDER victims in 2023 can be categorized as either reconnaissance targets or monetization targets. Reconnaissance targets are typically organizations in the business process outsourcing, customer relationship management, customer experience, technology and telecom sectors. SCATTERED SPIDER uses intrusions into these entities' networks to identify data that may prove useful in downstream, third-party monetization targeting.

The adversary's monetization target profile is considerably broader. Most directly observed targets include high-revenue — often Fortune 500 — U.S.-based private sector entities. A notable uptick in North American financial services victims occurred in the second half of 2023.

Law Enforcement Activity Targets BGH Adversaries

In 2023, various law enforcement agencies targeted BGH adversary operations and their supporting campaigns. Their actions ranged from arresting suspected adversary personnel to technically disrupting adversary infrastructure.

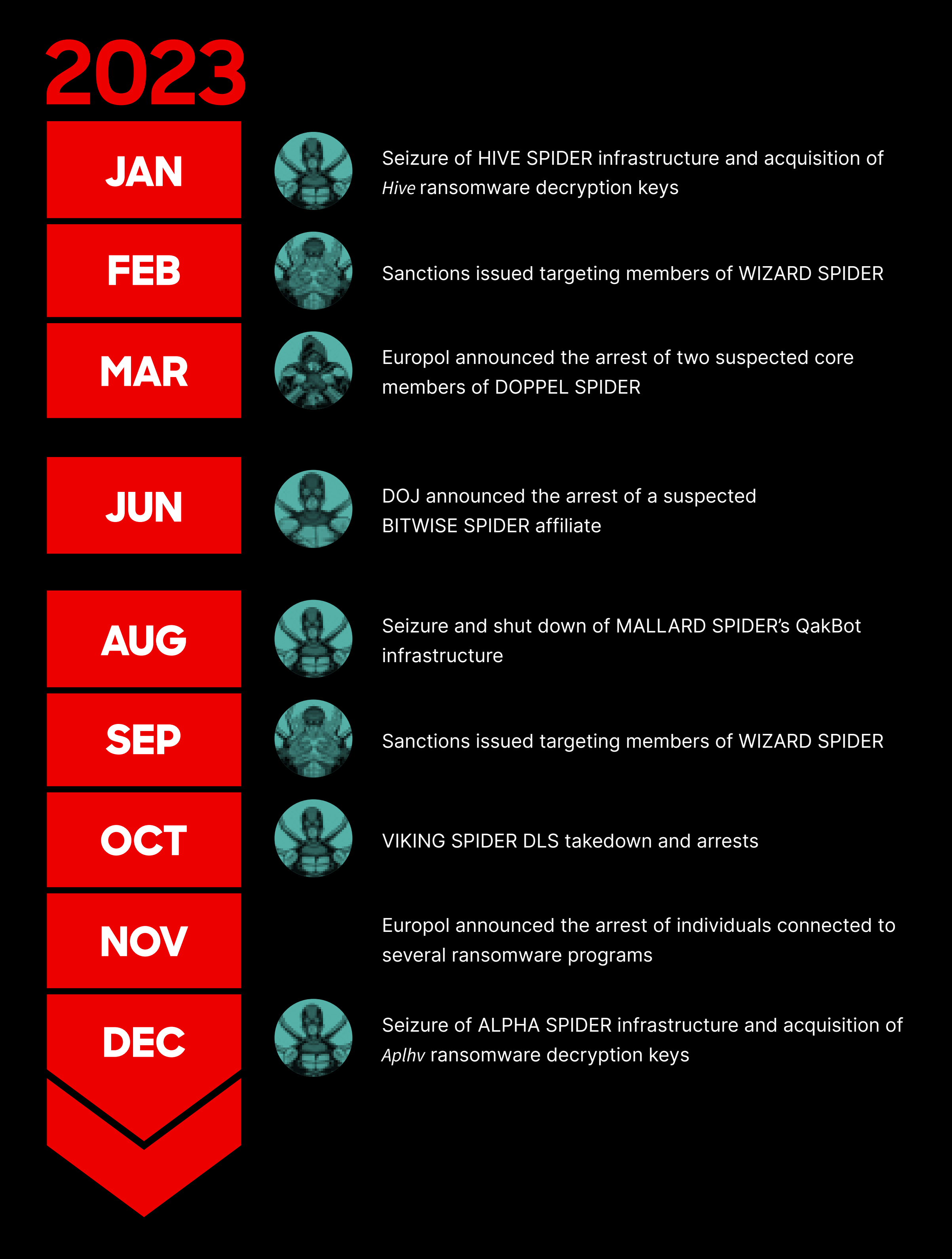


Figure 10. Law enforcement activity against BGH and supporting operations, 2023

In January 2023, a coordinated international law enforcement operation resulted in the seizure of HIVE SPIDER infrastructure and acquisition of the *Hive* ransomware decryption key. The U.S. Department of Justice (DOJ) has reportedly maintained access to HIVE SPIDER's internal infrastructure since July 2022 and has since provided decryption keys to more than 300 worldwide victims, preventing ransom payments totaling 130 million USD. No HIVE SPIDER activity has been observed since January 2023; however, *Hive* affiliates have since migrated to other ransomware as a service (RaaS) operations.

In February and September 2023, law enforcement issued sanctions against WIZARD SPIDER members aiming to restrict the named individuals' finances, travel, and assets and disrupt the adversary's operations as it worked to circumvent the restrictions.

In March 2023, Europol announced the arrest of two suspected core DOPPEL SPIDER members. In June 2023, the DOJ announced the arrest of a suspected BITWISE SPIDER affiliate. In August 2023, the FBI announced a multinational operation — using a custom payload to send a shutdown command — that removed MALLARD SPIDER's *QakBot* malware from more than 700,000 hosts and seized a significant amount of cryptocurrency. WANDERING SPIDER also used MALLARD SPIDER's *QakBot*.

In October 2023, law enforcement agencies announced they had taken down VIKING SPIDER's *Ragnar Locker* DLS and arrested a suspected *Ragnar Locker* developer. In November 2023, Europol also announced it had arrested personnel connected to an unnamed ransomware actor. Finally, in December 2023, the FBI seized ALPHA SPIDER's infrastructure, including the *Alphv* DLS — ransomware SCATTERED SPIDER used throughout most of 2023.

The FBI offered an *Alphv* decryption tool to more than 500 ALPHA SPIDER victims, prompting ALPHA SPIDER to migrate its DLS and affiliate panel to new Tor sites while it attempted to regain control of its compromised infrastructure. ALPHA SPIDER then removed targeting restrictions from affiliates, excepting prohibition against targeting entities within the Commonwealth of Independent States.

Data Theft and Extortion Optimization

Since 2019, BGH adversaries have threatened to publish stolen data on DLSs as a secondary extortion means in concert with deploying ransomware.[12] In 2023, adversaries continued to invent exploitation methods to steal victim data and increase pressure on victims, with many — including GRACEFUL SPIDER and MASKED SPIDER — adopting data theft as their sole means of extortion.

GRACEFUL SPIDER was the most prolific data theft and extortion actor in 2023. The adversary exploited zero-day vulnerabilities in file-transfer applications GoAnywhere Managed File Transfer and MOVEit Transfer as well as IT management software SysAid On-Premise. GRACEFUL SPIDER's *Clop* ransomware deployment within the scope of these campaigns was not observed, although the adversary exfiltrated and published data to its DLS that belonged to more than 380 victim organizations. To allow broader audience access to leaks, GRACEFUL SPIDER also published victim data on clearweb domains, a technique first used by an ALPHA SPIDER affiliate in 2022.

BGH adversaries have historically and indiscriminately exfiltrated and published stolen victim data. In 2023, these threat actors demonstrated greater focus on stolen data in efforts to maximize pressure on victims, as shown by the following:

- Publishing victim Domain Admin credentials and system IP addresses on the *Black Basta* RaaS DLS. This data could be leveraged by distinct threat actors to target victim organizations.
- Creating separate victim posts for third-party organizations whose data was identified in the victim network but were not subjected to compromises.
- Multiple RaaS affiliates compromised mental and physical healthcare entities and highlighted their access to — and provided previews of — sensitive data and records, including patient photos, in DLS posts.
- VICE SPIDER continued to use a PS script to automate data exfiltration but customized the script to search for directory and filenames containing strings such as `*violence*`, `*abuse*`, `*Theft*`, `*Stealing*`, `*humiliation*`, `*harassment*` and `*death*`, likely to identify data that posed a high potential for embarrassing victim organizations.

Many adversaries, including GRACEFUL SPIDER and MASKED SPIDER, have struggled with cryptographic flaws in their ransomware that enable trivial decryption under specific conditions. In contrast, data theft and extortion offer BGH actors an easier route to monetization, and many simply steal data from a single host or public-facing application. CrowdStrike CAO assesses that BGH adversaries will likely continue to become more targeted in their pursuit of data with a high potential for embarrassing victims.

---

12 https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

Outlook

The record number of victims named on DLSs throughout 2023 demonstrates BGH's status as the current most significant eCrime threat to organizations across all geographical regions and industries. This increase is driven by various factors, including GRACEFUL SPIDER's zero-day exploitation campaigns, BGH adversaries' continued targeting of unmanaged devices — such as edge gateway devices for initial access and targeting VMware ESXi for encryption — and an increasing number of adversaries naming victims following data theft incidents that did not include ransomware deployment.

Though CrowdStrike CAO assesses that ransomware will highly likely remain the primary extortion method through 2024, BGH adversaries will increasingly emphasize stolen-data exploitation as a means to pressure victims into payment. This is particularly true as U.S. Securities and Exchange Commission (SEC) rules impact major cybersecurity incident disclosures.[13]

SCATTERED SPIDER's *Alphv* ransomware underscored the effectiveness of extortion as a tactic throughout 2023. Though SCATTERED SPIDER previously monetized campaigns through cryptocurrency theft and SIM swaps, ransomware is a more opportunistic tactic, enabling the adversary to broaden its target scope. Barring any successful law enforcement activity targeting the adversary, SCATTERED SPIDER will highly likely remain a critical threat to high-revenue private sector entities in 2024, particularly those based in Europe and North America.

Coordinated international law enforcement operations targeted BGH actors in 2023. These included adversary personnel arrests, technical action against various capabilities, cryptocurrency seizure and sanctioning of named individuals. The disruption of HIVE SPIDER's *Hive* RaaS and MALLARD SPIDER's enabling *QakBot* malware left voids that were quickly filled by competing RaaS and malware as a service (MaaS) actors, demonstrating the eCrime ecosystem's resilience against takedowns that do not arrest the individuals behind the operations.



THE RECORD NUMBER OF VICTIMS NAMED ON DLSs THROUGHOUT 2023 DEMONSTRATES BGH'S STATUS AS THE CURRENT MOST SIGNIFICANT ECRIME THREAT TO ORGANIZATIONS ACROSS ALL GEOGRAPHICAL REGIONS AND INDUSTRIES.

13 https://www.sec.gov/news/press-release/2023-139

eCRIME ENABLERS

Malware Delivery Trends Following Mark-of-the-Web Patch on ISO Files

Adversaries in 2023 experimented with malware delivery methods that do not rely on macros or ISO files, following a sharp increase in ISO files being used for malware delivery and a subsequent patch by Microsoft for a Mark-of-the-Web bypass vulnerability in container files in 2022.

The number of malware campaigns using malicious OneNote files for initial access rose significantly[14] between late December 2022 and March 2023, with the technique's earliest adopters including criminals distributing information stealers and commodity malware. By mid-January 2023, large-scale malware distributors such as LUNAR SPIDER, HONEY SPIDER and MALLARD SPIDER began using OneNote files as a primary malware distribution method. In March 2023, Microsoft announced a change that would prevent file types commonly abused by adversaries from being embedded in OneNote files.[15] Following the announcement, the popularity of OneNote files within adversary campaigns rapidly declined.

Though no one technique has emerged as a front-runner to replace OneNote files, adversaries continue to experiment with malware delivery methods. Adversaries such as LUNAR SPIDER, APOTHECARY SPIDER and HERMIT SPIDER have consistently used malvertising and search engine optimization (SEO) poisoning.

Adversaries reliant on spam campaigns use multiple techniques and file types to deliver malware. Several adversaries have used PDF files containing links to files hosted on external URLs as well as HTML smuggling. More novel techniques have included using WebDAV files to distribute payloads. Toward the end of 2023, multiple malware families were distributed in new lures containing fake browser updates.

Malvertising and SEO Poisoning

Malvertising is a technique in which threat actors create malicious advertisements to facilitate criminal activity. Adversaries use SEO poisoning to falsely promote malicious websites to higher ranks in search engine results. Similar to malvertising, SEO poisoning relies on users believing the results closest to the top of a search result are the most credible.

Throughout 2023, adversaries such as LUNAR SPIDER regularly abused Google advertisements to ensure their malicious ads appeared at the top of search result pages. Threat actors such as SolarMarker operators regularly used SEO poisoning throughout 2023.

---

14 https://www.crowdstrike.com/blog/qakbot-ecrime-campaign-leverages-microsoft-onenote-for-distribution/
15 https://learn.microsoft.com/en-us/deployoffice/security/onenote-extension-block

Increasing macOS Malware Use

Throughout 2023, multiple macOS malware variants — including *MacOS Stealer, Private MacOS Stealer, ShadowVault* and COOKIE SPIDER's *Atomic macOS Stealer (AMOS)* — emerged on underground marketplaces. All observed macOS malware families are information stealers capable of harvesting stored passwords, cookies and cryptocurrency wallets.

AMOS customers have distributed these tools via SEO poisoning as well as fake play-to-earn games and illegitimate job advertisements. *MacOS Stealer* customers, including BITWISE SPIDER, ROYAL SPIDER and ALPHA SPIDER ransomware affiliates, have praised the stealer. Although COOKIE SPIDER stated that a portion of its current 50 to 100 customers include BITWISE SPIDER and ALPHA SPIDER affiliates, CrowdStrike CAO cannot presently verify this claim.

macOS stealers gained traction in the eCrime ecosystem throughout 2023 due to their ability to enable opportunistic actors and ransomware affiliates during criminal operations. Since the majority of information stealers typically target Windows-based OSs, the increasing number of macOS stealers in the eCrime ecosystem has expanded eCrime profit opportunities.

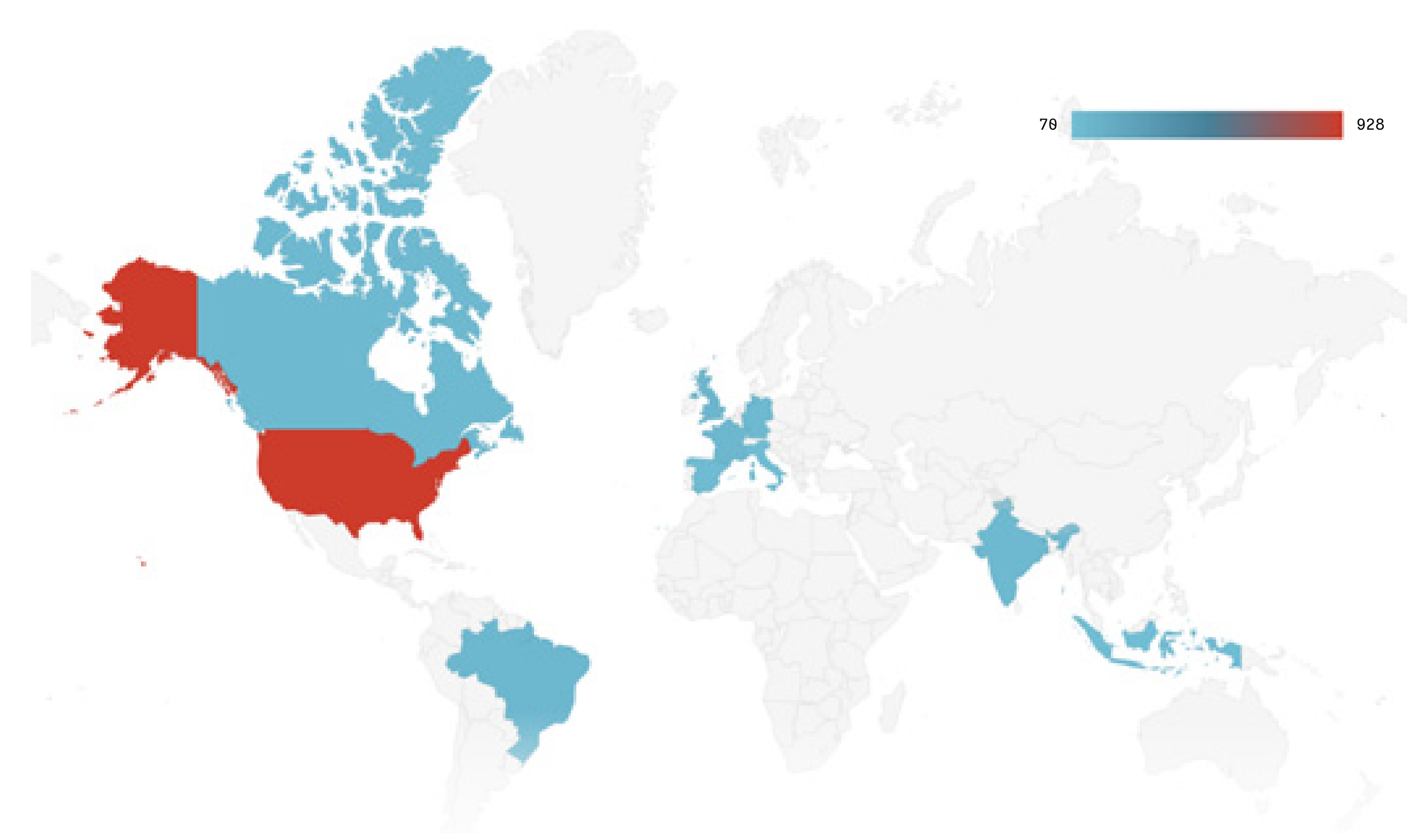
Access Brokers Persistently Provide Access Opportunities

Access brokers continued to profit from providing initial access to a variety of eCrime threat actors in 2023, with the number of accesses advertised increasing by 20% compared to 2022. The academic sector was the most frequently advertised, and advertisements for U.S.-based entities far surpassed all other regions. Initial access TTPs observed in 2023 were relatively consistent with those used in 2022 and regularly targeted and abused compromised credentials.



ACCESS BROKERS CONTINUED TO PROFIT FROM PROVIDING INITIAL ACCESS TO A VARIETY OF eCRIME THREAT ACTORS IN 2023, WITH THE NUMBER OF ACCESSES ADVERTISED INCREASING BY 20% COMPARED TO 2022.

TOP ACCESS BROKER ADVERTISEMENTS BY COUNTRY
2023



TOP SECTORS ADVERTISED BY ACCESS BROKERS | 2023

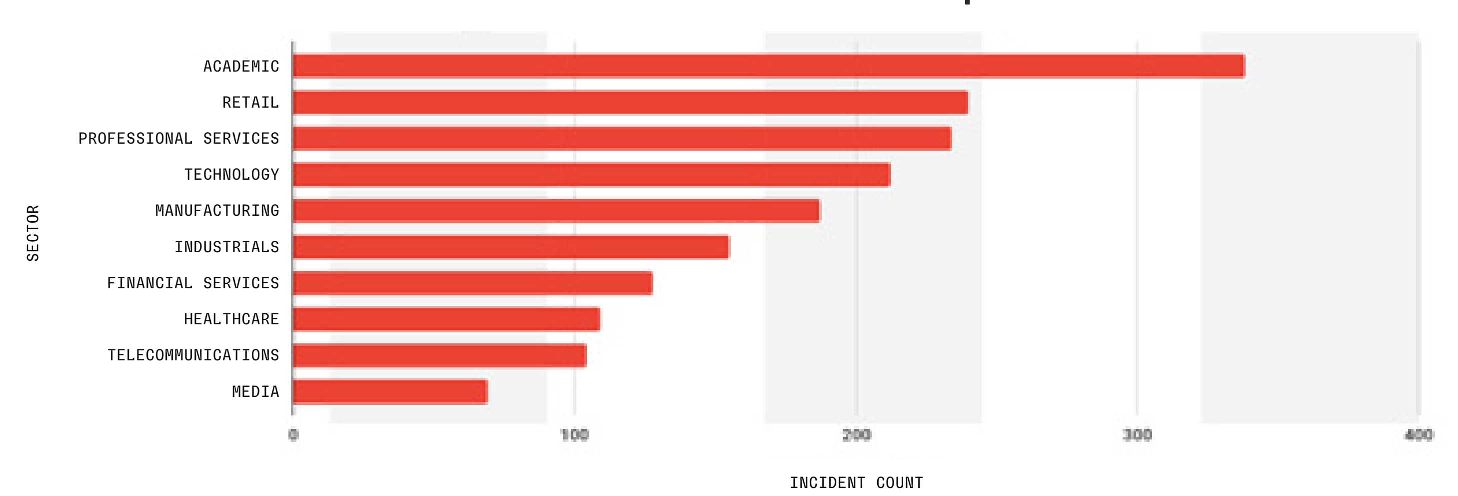


Figure 11. Top 10 countries and sectors advertised by access brokers, 2023

Outlook

The rise of macOS malware and the evolution of malware delivery techniques demonstrate the eCrime ecosystem's innovative nature. Furthermore, eCrime enablers regularly copy successful tactics used by other criminal actors, as made evident by the increase of OneNote files for malware delivery.

eCrime enablers will highly likely continue to innovate and offer new products on criminal marketplaces in 2024. This assessment is made with high confidence based on historical trends in the eCrime ecosystem. Malware delivery trends will likely continue to fluctuate, with SEO poisoning and malvertising remaining popular and spam-reliant adversaries proceeding to regularly experiment with different methods. This assessment is made with high confidence based on malware delivery trends observed since the end of 2022.

The access broker threat shows no immediate sign of abating. These threat actors will almost certainly facilitate intrusions into various organizations worldwide throughout 2024 using a mixture of established TTPs alongside commodity and custom tooling.

TARGETED eCRIME

Adversaries Continue Legitimate RMM Tool Use

Throughout 2023, multiple targeted eCrime adversaries — particularly CHEF SPIDER, DISTANT SPIDER and SOLAR SPIDER — heavily used legitimate remote monitoring and management (RMM) tools.

Starting in March 2023, CHEF SPIDER adopted sophisticated social engineering tactics to direct victims to download Inno Setup and ClickOnce installers for RMM tool ConnectWise ScreenConnect. Though CHEF SPIDER has historically targeted point-of-sale systems in the hospitality sector by compromising internet-facing servers, the adversary gradually shifted to targeting U.S.-based hospitality sector service providers, financial service providers and digital marketing firms throughout 2023.

In 2023, DISTANT SPIDER — which universally relies on ConnectWise ScreenConnect — continued deploying MSI installers (aka Windows Installers) for this legitimate RMM tool after exploiting vulnerable internet-facing servers within victim environments. In September 2023, an earlier DISTANT SPIDER ConnectWise ScreenConnect intrusion likely enabled an ALPHA SPIDER affiliate to exfiltrate data and demand a ransom from a victim.

In June 2023, SOLAR SPIDER likely used phishing emails to direct victims to download a ZIP archive hosted on GitHub. This archive contained a loader that abuses DLL search-order hijacking to run the legitimate RMM Remote Management System tool. SOLAR SPIDER has used the legitimate RMM tool NetSupport Manager since at least October 2022.

Historical CARBON SPIDER Malware Distributed in Low-Volume Campaigns

Throughout 2023, eCrime actors used numerous malware families previously exclusive to CARBON SPIDER (Figure 12). Since the now-inactive MaaS vendor *Goodsoft* distributed these families in 2022 and 2023, none of these campaigns can be attributed to now-inactive CARBON SPIDER; however, the campaigns demonstrate the tools' enduring popularity. In contrast to typical MaaS operators, the low volume of campaigns using *Goodsoft* tooling likely indicates only a handful of customers were given access.

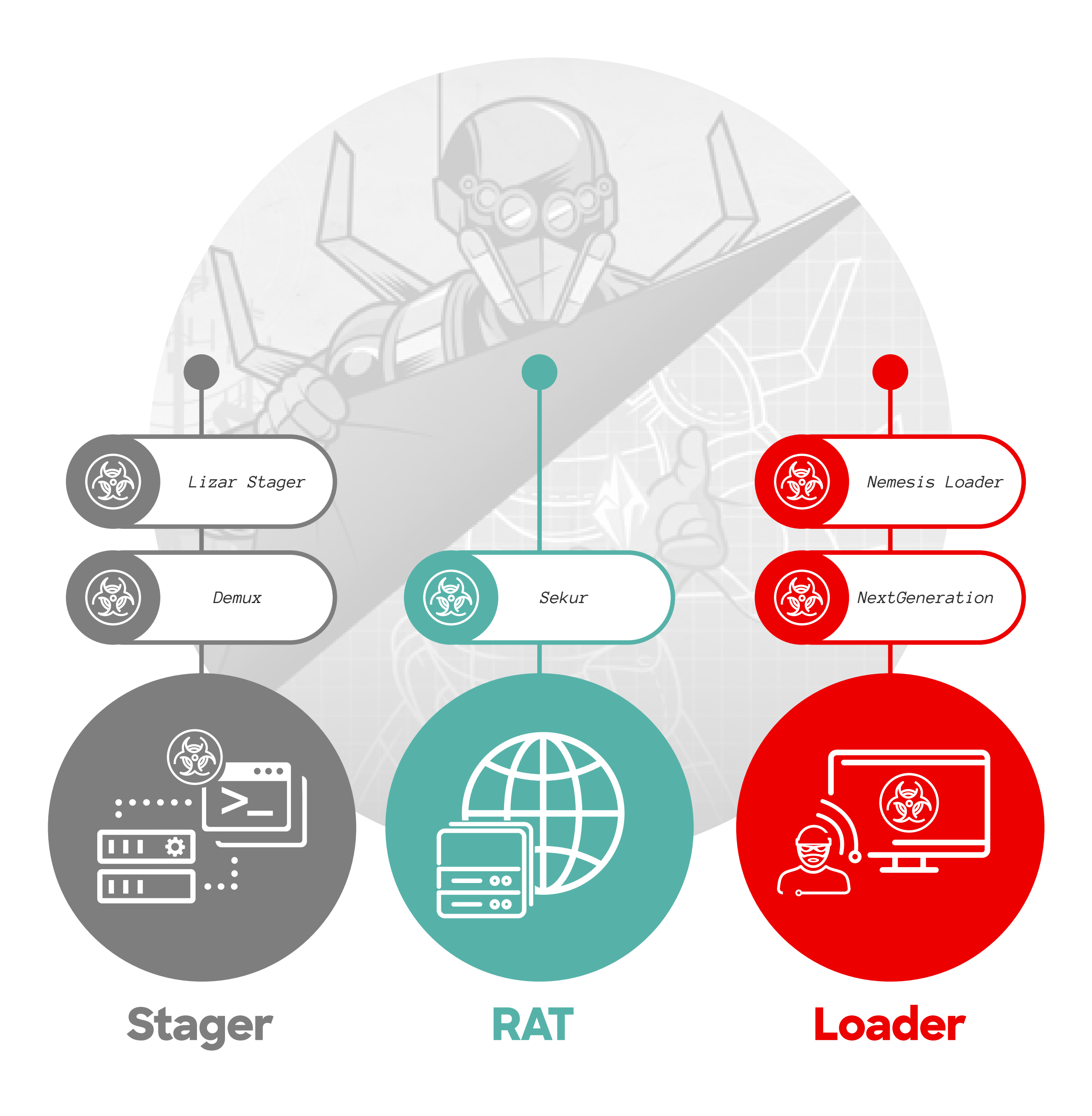


Figure 12. Legacy CARBON SPIDER tooling used in 2023

Additional LATAM-Focused Adversaries Identified

In 2023, CrowdStrike CAO named three new SPIDER adversaries focused primarily — but not exclusively — on Latin America (LATAM): ODYSSEY SPIDER, ROBOT SPIDER and SQUAB SPIDER (Figure 13). Including previously identified BLIND SPIDER, four SPIDER adversaries now focus on LATAM targeting.

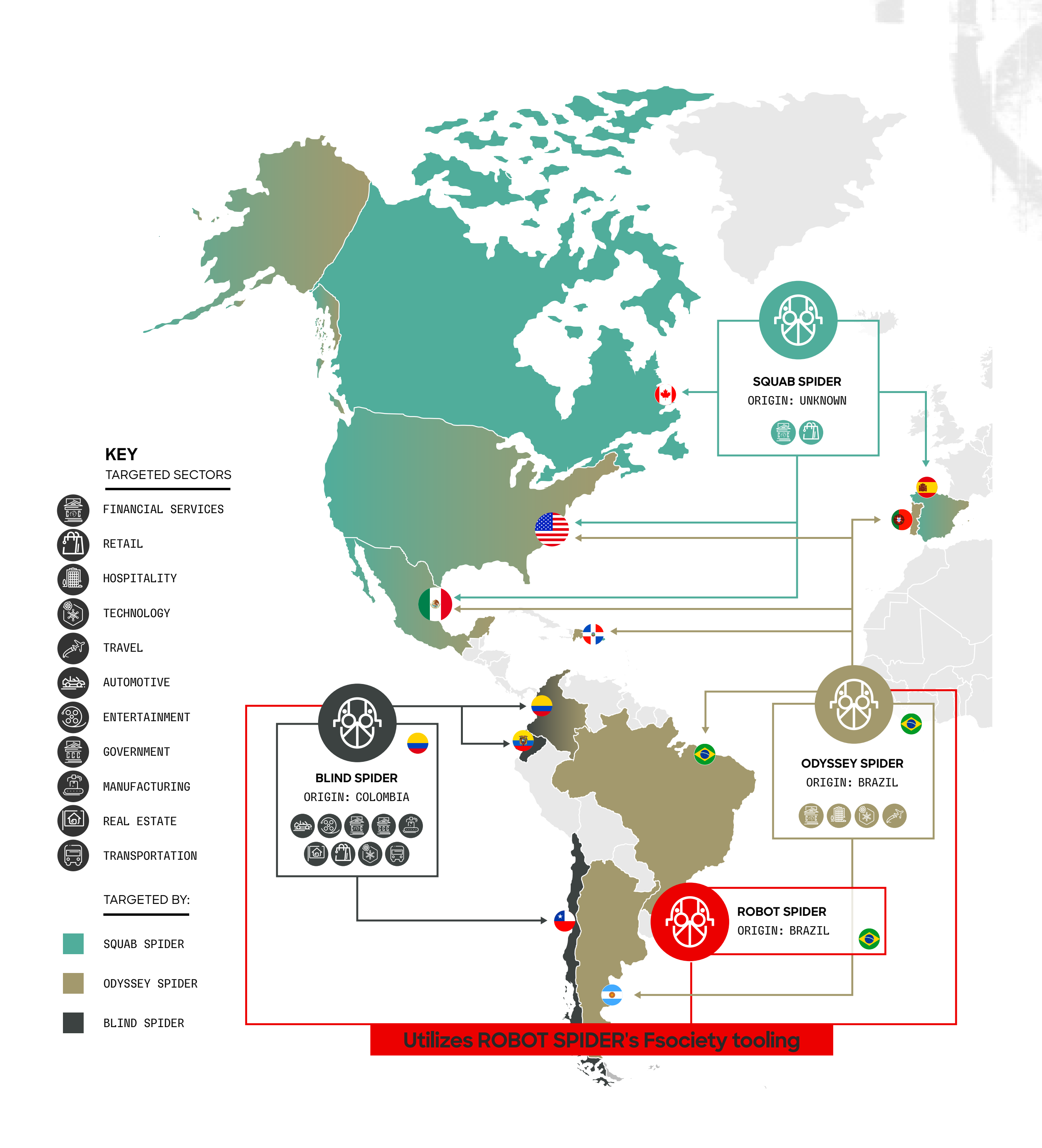


Figure 13. LATAM-focused SPIDER adversaries

AVIATOR SPIDER, BLIND SPIDER and ODYSSEY SPIDER all used ROBOT SPIDER's *Fsociety* crypter service during 2023. *Fsociety* tools typically consist of a set of scripts that download and execute an intermediate .NET payload that subsequently loads a final RAT payload in memory. Throughout 2023, ROBOT SPIDER continued to update the *Fsociety* crypter to improve obfuscation and add capabilities. Generally, infection chains leveraging *Fsociety* culminated in commodity RATs such as *njRAT Lime*.

ODYSSEY SPIDER, which is likely based in Brazil, uses ROBOT SPIDER's *Fsociety* crypter service along with other commodity crypters and RATs. ODYSSEY SPIDER predominantly focuses on the travel and hospitality sectors in LATAM and Southeastern Europe, specifically aiming to monetize payment card details entered during travel-related booking processes. However, in Q3 2023, the adversary began targeting numerous other sectors and regions, likely while leveraging local tax return periods.

SQUAB SPIDER primarily targets financial institutions, particularly but not exclusively those based in Mexico. The adversary achieves initial access by exploiting web servers to deploy a wide set of webshells. From there, threat actors rely on passive BLUEAGAVE bind shells or simple listeners to enable lateral movement through a network and to generally avoid conventional C2 traffic. SQUAB SPIDER likely attempts to steal transaction-related data from victims.

Outlook

Though opportunistic BGH campaigns remain the primary eCrime threat across all sectors, a smaller eCrime actor subset will likely continue targeted eCrime campaigns seeking to steal payment card- or transaction-related data from victims. As with the BGH ecosystem, legitimate RMM tools will likely remain popular among targeted eCrime operations due to their widespread use within normal business processes. The endurance of LATAM-focused adversaries BLIND SPIDER, ODYSSEY SPIDER, ROBOT SPIDER and SQUAB SPIDER highlights how the LATAM-targeted eCrime ecosystem will likely persist in the mid-term.



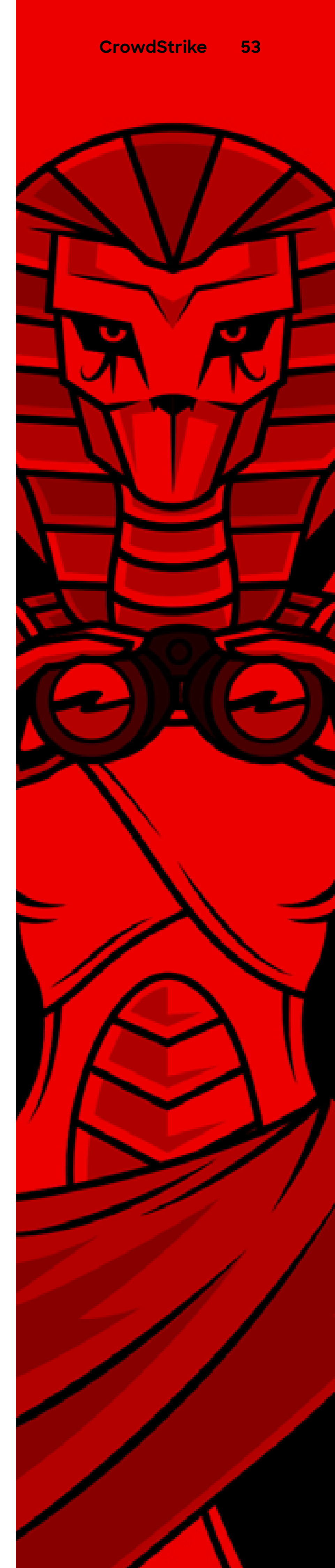
Conclusion

Over the course of 2023, CrowdStrike CAO observed adversaries across the targeted intrusion, eCrime and hacktivist landscapes operating with unprecedented stealth. The ability to operate undetected remains paramount for malicious actors, and today's sophisticated cybercriminals continue to discover new methods to increase effectiveness, enhance operations and achieve objectives.

eCrime remained a 2023 threat landscape cornerstone, with BGH adversaries SCATTERED SPIDER and GRACEFUL SPIDER accounting for most activity. CrowdStrike CAO assesses BGH will continue to pose the dominant threat within the eCrime landscape in 2024. This assessment is made with high confidence based on the continued success of these operations, as observed in the 76% growth in DLS posts in 2023. Trends likely to be observed in 2024 in support of BGH operations include ransomware-free data leak operations and an increase in cloud-conscious operations.

The number of cloud-conscious threat actors continued to grow in 2023 — as in 2022 — and will highly likely continue to grow in 2024. Adversaries are highly motivated to invest in and use cloud and other new technologies, such as generative AI, to increase the efficiency and success of their operations. Cloud-aware adversaries will look to detect, enumerate and navigate cloud environments to harvest valuable proprietary information from Microsoft 365, SharePoint and code repositories. They will use this information in ongoing operations and ransom negotiations or simply sell it to other eCrime adversaries.

Financially motivated adversaries also increasingly realized the benefits of dedicated relationships in 2023 and were likely able to increase resulting operational success rates. Access brokers and RaaS actors will likely continue to forge dedicated relationships in 2024. The coming year will also likely include enhancements in social engineering effectiveness, MFA bypass and third-party provider targeting in efforts to leverage a single larger point of access.



High-profile geopolitical conflicts — namely the Russia-Ukraine and Israel-Hamas conflicts — generated significant targeted intrusion and hacktivist cyber activity in 2023, particularly for Iran-nexus and Russia-nexus adversaries. In 2024, these and other high-profile conflicts will remain as significant hacktivism drivers.

Beyond cyber activity related to the Israel-Hamas conflict, Iran-nexus adversaries remained consistent in targeting telecom organizations, a trend likely to continue in 2024. Russia-nexus adversaries also persisted in their targeting of Ukraine, NATO members and partner countries. They will almost certainly continue to conduct intelligence collection operations and IO in these geographies in 2024.

CrowdStrike CAO graduated several activity clusters to named adversaries in 2023, including the first-ever Egypt-nexus adversary, WATCHFUL SPHINX. Consistent with previous assessments, CrowdStrike CAO expects the majority of established adversaries and activity clusters to continue to expand or update their capabilities in 2024. Fewer adversaries and activity clusters around the world are likely to expand their assessed target scope; rather, they will likely continue to focus on historical and predominantly regional target sets.

Within the vulnerability threat landscape, CrowdStrike CAO assesses that several 2023 trends — namely, edge device and EOL product targeting — will persist in 2024. eCrime threat actors remained the primary threat to most mobile users in 2023 and will likely continue as such in 2024. Targeted intrusion actors will also almost certainly continue to target mobile devices, with increases in platform and device security causing less sophisticated adversaries to struggle to operate successfully in that space.

With the creation of Counter Adversary Operations, CrowdStrike remains steadfast in its mission to stop breaches. Combining best-in-class threat intelligence with a professional, managed threat hunting service unlike anything else offered in the industry, CrowdStrike ensures its customers can access industry-leading information to drive their individual operational success.

CrowdStrike CAO remained focused on disrupting the adversary in 2023 and will continue to deliver unparalleled threat intelligence in 2024 and beyond.

Recommendations

1 Make identity protection a must-have

Due to high success rates, identity-based and social engineering attacks surged in 2023. Stolen credentials grant adversaries swift access and control — an instant gateway to a breach. To counter these threats, it is essential to implement phishing-resistant multifactor authentication and extend it to legacy systems and protocols, educate teams on social engineering and implement technology that can detect and correlate threats across identity, endpoint and cloud environments. Cross-domain visibility and enforcement enables security teams to detect lateral movement, get full attack path visibility and hunt for malicious use of legitimate tools. Addressing sophisticated access methods such as SIM swapping, MFA bypass and the theft of API keys, session cookies and Kerberos tickets requires proactive and continuous hunting for malicious behavior.

2 Prioritize cloud-native application protection platforms (CNAPPs)

Cloud adoption is exploding as companies realize the potential for innovation and business agility that the cloud offers. Due to this growth, the cloud is rapidly becoming a major battleground for cyberattacks. Businesses need full cloud visibility, including into applications and APIs, to eliminate misconfigurations, vulnerabilities and other security threats. CNAPPs are critical: Cloud security tools shouldn't exist in isolation, and CNAPPs provide a unified platform that simplifies monitoring, detecting and acting on potential cloud security threats and vulnerabilities. Select a CNAPP that includes pre-runtime protection, runtime protection and agentless technology to help you discover and map your apps and APIs running in production, showing you all attack surfaces, threats and critical business risks.

3 Gain visibility across the most critical areas of enterprise risk

Adversaries often use valid credentials to access cloud-facing victim environments and then use legitimate tools to execute their attack, making it difficult for defenders to differentiate between normal user activity and a breach. To identify this type of attack, you need to understand the relationship between identity, cloud, endpoint and data protection telemetry, which may be in separate systems. In fact, the average enterprise uses 45+ security tools, creating data silos and gaps in visibility. By consolidating into a unified security platform with AI capabilities, organizations have complete visibility in one place and can easily control their operations. With a consolidated security platform, organizations save time and money and can quickly and confidently discover, identify and stop breaches.



Drive efficiency: Adversaries are getting faster — are you?

It takes adversaries an average of 62 minutes — and the fastest only 2 minutes — to move laterally from an initially compromised host to another host within the environment. Can you keep up? Let's face it — legacy SIEM solutions have failed the SOC. They are too slow, complex and costly, and they were designed for an age when data volumes — and adversary speed and sophistication — were a fraction of what they are today. You need a tool that's faster, easier to deploy and more cost-effective than legacy SIEM solutions. Investigate better approaches, such as CrowdStrike Falcon® Next-Gen SIEM, which unifies all threat detection, investigation and response in one cloud-delivered, AI-native platform for unrivaled efficiency and speed. Or, if you don't have an internal SOC team, consider 24/7 managed detection and response (MDR).

5

Build a cybersecurity culture

Though technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

CrowdStrike Products and Services

Endpoint Security

FALCON PREVENT | NEXT-GENERATION ANTIVIRUS

Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

FALCON INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

Offers industry-leading, unified EDR and extended detection and response (XDR) with enterprise-wide visibility to automatically detect adversary activity and respond across endpoints and all key attack surfaces

FALCON COMPLETE | MANAGED DETECTION AND RESPONSE

Stops and eradicates threats in minutes with 24/7 expert management, monitoring and surgical remediation, proactive threat hunting, and integrated threat intelligence — all backed by the industry's strongest Breach Prevention Warranty

FALCON COMPLETE XDR | MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

Expands Falcon Complete's industry-leading MDR service with cross-domain XDR protection run by CrowdStrike's elite 24/7 expertise, proactive threat hunting and native threat intelligence

FALCON FIREWALL MANAGEMENT | HOST FIREWALL

Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

FALCON DEVICE CONTROL | USB SECURITY

Provides the visibility and precise control required to enable safe usage of USB devices across your organization

FALCON FOR MOBILE | ENDPOINT DETECTION AND RESPONSE

Protects against threats to iOS and Android devices, extending XDR/EDR capabilities to your mobile devices, with advanced threat protection and real-time visibility into app and network activity

Counter Adversary Operations

FALCON ADVERSARY OVERWATCH™ | UNIFIED THREAT HUNTING

Provides around-the-clock protection across endpoint, identity and cloud workloads delivered by AI-powered threat hunting experts, and includes built-in threat intelligence to expose adversary tradecraft, vulnerabilities and stolen credentials

FALCON ADVERSARY INTELLIGENCE | SOC AUTOMATION

Cuts response time from days to minutes across the entire security stack with end-to-end intelligence automation, and enables you to instantly submit potential threats to an automated sandbox, extract indicators of compromise and deploy countermeasures — all while continuously monitoring for fraud and safeguarding your brand, employees and sensitive data

FALCON ADVERSARY HUNTER | INTEL-LED THREAT HUNTING

Provides world-class intelligence reporting, technical analysis, and threat hunting and detection libraries, and cuts the time and cost required to understand and defend against sophisticated nation-state, eCrime and hacktivist adversaries

FALCON COUNTER ADVERSARY OPERATIONS ELITE
ON-DEMAND ANALYST

Provides an assigned analyst who uses advanced investigative and threat hunting tools powered by deep adversary intelligence to identify and disrupt adversaries across your IT environment and beyond

Cloud Security

FALCON CLOUD SECURITY

Provides breach protection, including threat intelligence, detection and response; workload runtime protection; and cloud security posture management across AWS, Azure and Google Cloud Platform (GCP)

FALCON CLOUD SECURITY FOR CONTAINERS

Delivers cloud and container security and breach protection; cloud security posture management; threat detection and response across on-premises, hybrid and multi-cloud environments; and cloud workload protection, including container security and Kubernetes protection

FALCON CLOUD SECURITY FOR MANAGED CONTAINERS

Provides cloud and container security, including threat intelligence, detection and response; container image security; and Kubernetes protection

FALCON OVERWATCH CLOUD THREAT HUNTING

MANAGED SERVICES

Unearths cloud threats, from unique cloud attack paths with complex trails of cloud IOAs and indicators of misconfiguration (IOMs) to well-concealed adversary activity in your critical cloud infrastructure — including AWS, Azure and GCP

FALCON COMPLETE CLOUD SECURITY

MDR FOR CLOUD WORKLOADS

Provides a fully managed cloud workload protection service, delivering 24/7 expert security management, threat hunting, monitoring and response for cloud workloads, backed by CrowdStrike's industry-leading Breach Prevention Warranty

Identity Protection

FALCON IDENTITY THREAT DETECTION

Enables hyper-accurate detection of identity-based threats in real time, leveraging AI and behavioral analytics to provide deep actionable insights to stop modern attacks like ransomware

FALCON IDENTITY THREAT PROTECTION

Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

FALCON COMPLETE IDENTITY THREAT PROTECTION

MANAGED IDENTITY THREAT PROTECTION

Provides a fully managed identity protection solution delivering frictionless, real-time identity threat prevention and IT policy enforcement, monitoring and remediation — powered 24/7 by CrowdStrike's team of experts

Security and IT Operations

FALCON DISCOVER | IT HYGIENE

Identifies unauthorized accounts, systems and applications anywhere in your environment in real time, enabling instant visibility to improve your overall security posture

FALCON SPOTLIGHT | VULNERABILITY MANAGEMENT

Offers security teams an automated, comprehensive vulnerability management solution, enabling faster prioritization and integrated remediation workflows without resource-intensive scans

FALCON EXPOSURE MANAGEMENT | EXPOSURE MANAGEMENT

Allows security teams to prioritize exposures making the biggest impact and proactively reduce an adversary's opportunity for compromise and lateral movement

FALCON SURFACE | EXTERNAL ATTACK SURFACE MANAGEMENT

Continuously discovers and maps all internet-facing assets to shut down potential exposure with guided mitigation plans to reduce the attack surface

FALCON DATA PROTECTION | UNIFIED DATA PROTECTION

Provides deep real-time visibility into what is happening with sensitive data and stops data theft with policy enforcement that automatically follows content, not files

FALCON FILEVANTAGE | FILE INTEGRITY MONITORING

Provides real-time, comprehensive and centralized visibility that boosts compliance and offers relevant contextual data

FALCON FORENSICS | FORENSIC CYBERSECURITY

Automates collection of point-in-time and historic forensic triage data for robust analysis of cybersecurity incidents

FALCON FOR IT | AUTOMATED WORKFLOWS

Extends the Falcon platform to automate IT and security workflows with an end-to-end, visibility-to-action life cycle

Next-Gen SIEM

FALCON NEXT-GEN SIEM | SIEM AND LOG MANAGEMENT

Empowers you to swiftly shut down adversaries and slash SOC costs by unifying industry-leading detection, world-class intelligence, blazing-fast search and AI-led investigations in one cloud-delivered platform

CrowdStrike Services

INCIDENT RESPONSE

Stop active breaches and restore order with the most informed and capable IR team available

- Incident Response
- Compromise Assessment
- Endpoint Recovery
- Network Detection Services
- Services Retainer

STRATEGIC ADVISORY SERVICES

Develop and mature the security program to improve defenses

- Tabletop Exercise
- Maturity Assessment
- Ransomware Defense Assessment
- SOC Assessment
- SEC Readiness
- Board and CXO Briefings

RED TEAM SERVICES

Stress-test and validate defenses through simulated attacks

- Penetration Testing
- Red Team/Blue Team Exercise
- Adversary Emulation Exercise

CLOUD AND IDENTITY SERVICES

Proactively secure the new perimeter

- Identity Security Assessment
- Cloud Security Assessment
- Red Team/Blue Team Exercise for Cloud
- Cloud Compromise Assessment

TECHNICAL ADVISORY SERVICES

Audit and address security gaps to tangibly reduce risk

- Technical Risk Assessment
- Cyber Threat Risk Evaluation

TRAINING AND SECURITY UPSKILLING

Become security experts under CrowdStrike tutelage

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: www.crowdstrike.com/free-trial-guide